View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Calhoun, Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2015-03

Crowdsourcing intelligence to combat terrorism: harnessing bottom-up collection to prevent lone-wolf terror attacks

Coultas, Bryan T.

Monterey, California: Naval Postgraduate School

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CROWDSOURCING INTELLIGENCE TO COMBAT TERRORISM: HARNESSING BOTTOM-UP COLLECTION TO PREVENT LONE-WOLF TERROR ATTACKS

by

Bryan T. Coultas

March 2015

Thesis Advisor: Erik Dahl
Second Reader: Naazneen Barma

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2015	Master's Thesis

4. TITLE AND SUBTITLE
CROWDSOURCING INTELLIGENCE TO COMBAT TERRORISM: HARNESSING BOTTOM-UP COLLECTION TO PREVENT LONE-WOLF TERROR ATTACKS

5. FUNDING NUMBERS

6. AUTHOR(S) Bryan T. Coultas

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943–5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

U.S. officials have acknowledged that attackers of the lone-wolf and isolated-cell organizational type are on the rise and now pose a greater threat than major coordinated actions. Traditional intelligence methods, using a top-down approach with an emphasis on signals intelligence, are ill-equipped to identify and prevent terrorists using lone-wolf tactics.

Crowdsourcing, as a problem-solving technique, is a relatively new idea but has shown great promise in tackling issues similar to the identification of lone-wolf terrorists. At its core, crowdsourcing is a method for thousands or even millions of people to contribute their knowledge, expertise, or skills towards a unified task. Done correctly, it has produced results unachievable by traditional tasking of humans or computers.

This thesis identifies how the signals surrounding lone-wolf attacks are different and more subtle in nature from those mounted by organized terror groups. In turn, the thesis examines the potential benefits of crowdsourcing intelligence in order to strengthen the U.S. intelligence community's ability to approach this emerging problem of lone-wolf terrorism. In short, this thesis proposes that the U.S. intelligence community harness the power of U.S. citizens to help prevent identify the subtle indictors presented by lone-wolf terrorists in order to prevent lone-wolf terrorist attacks.

14. SUBJECT TERMS
lone-wolf, terrorism, crowdsource, crowdsourcing, domestic intelligence, big data, distributed network, citizen participation

15. NUMBER OF PAGES
95

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CROWDSOURCING INTELLIGENCE TO COMBAT TERRORISM: HARNESSING BOTTOM-UP COLLECTION TO PREVENT LONE-WOLF TERROR ATTACKS

Bryan T. Coultas
Lieutenant Commander, United States Navy
B.A., The University of Texas, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2015**

Author: Bryan T. Coultas

Approved by: Erik Dahl
Thesis Advisor

Naazneen Barma
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

U.S. officials have acknowledged that attackers of the lone-wolf and isolated-cell organizational types are on the rise and now pose a greater threat than major coordinated actions. Traditional intelligence methods, using a top-down approach with an emphasis on signals intelligence, are ill-equipped to identify and prevent terrorists using lone-wolf tactics.

Crowdsourcing, as a problem-solving technique, is a relatively new idea but has shown great promise in tackling issues similar to the identification of lone-wolf terrorists. At its core, crowdsourcing is a method for thousands or even millions of people to contribute their knowledge, expertise, or skills toward a unified task. Done correctly, it has produced results unachievable by traditional tasking of humans or computers.

This thesis identifies how the signals surrounding lone-wolf attacks are different and more subtle in nature from those mounted by organized terror groups. In turn, the thesis examines the potential benefits of crowdsourcing intelligence in order to strengthen the U.S. intelligence community's ability to approach this emerging problem of lone-wolf terrorism. In short, this thesis proposes that the U.S. intelligence community harness the power of U.S. citizens to help prevent identify the subtle indictors presented by lone-wolf terrorists in order to prevent lone-wolf terrorist attacks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AQAP	Al-Qaeda in the Arabian Peninsula
AQI	Al-Qaeda in Iraq
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DHS	United States Department of Homeland Security
FBI	Federal Bureau of Investigation
HUMINT	human intelligence
IARPA	Intelligence Advanced Research Projects Activity
MTURK	Amazon's Mechanical Turk
NSA	National Security Agency
OSINT	open-source intelligence
SIGINT	signals intelligence
SOCMINT	social media intelligence

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Erik Dahl for the mentorship and professional analysis he has provided to me and my thesis. His insight into lone-wolf terrorism and domestic intelligence were of enormous benefit to this thesis.

I would like to thank Dr. Naazneen Barma for her insight and alternative viewpoint for my thesis. She provided an excellent sounding board in an effort to sanity-check the hypotheses and conclusions presented in this thesis

I would also like to thank my wife, Jen, for her steadfast love and support throughout the writing of this thesis and during my continued service in the military. Her proofreading and feedback as a layperson were invaluable in the writing of this thesis.

Finally, I would like to thank my cat, Ellie, who ensured a warm lap throughout the entire writing process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. PREVENTING LONE-WOLF TERRORISM: INTRODUCTION

A. MAJOR RESEARCH QUESTION

The large hierarchical terrorist groups such as Al-Qaeda have been fractured and their power has greatly lessened thanks largely to efforts by American law enforcement and military organizations. But several U.S. officials have openly acknowledged that attackers of the lone-wolf or isolated-cell organizational type are on the rise and now pose a more serious threat than major coordinated actions. President Obama himself said that "a 'lone-wolf' terror attack in the United States is more likely than a major coordinated effort like the Sept. 11 attacks nearly a decade ago."[1]

Traditional intelligence methods, using a top-down approach with an emphasis on signals intelligence (SIGINT), are ill-equipped to identify and prevent terrorists using lone-wolf tactics. According to former Homeland Security Secretary Janet Napolitano, "We are also seeing a rise of activities by individuals who are actually in the country, and they are acting by themselves and that kind of attack is the most difficult to prevent because there is nothing to intercept."[2]

Crowdsourcing, as a problem-solving technique, is a relatively new idea but one that has shown great promise in tackling issues similar to the identification of lone-wolf terrorists. At its core, crowdsourcing is a method for thousands or even millions of people to contribute their knowledge, expertise, or skills towards a unified task. Done correctly, it has produced results unachievable by traditional tasking of humans or computers.

This thesis focuses on identifying how the signals surrounding lone-wolf attacks are different in nature from those mounted by organized terror groups. In turn, the thesis examines the potential benefits of crowdsourcing intelligence in order to strengthen the

[1] Associated Press, "Obama: 'Lone Wolf' Terror Attack More Likely Than Major Coordinated Effort," *The Huffington Post*, August 16, 2011, http://www.huffingtonpost.com/2011/08/16/obama-lone-wolf-terror_n_928880.html.

[2] Trish Turner and The Associated Press, "Napolitano: 'Lone Wolf' Terrorists On the Rise, Most Difficult to Intercept," *Fox News*, August 17, 2011, http://www.foxnews.com/politics/2011/08/17/obama-lone-wolf-terror-strike-biggest-concern/.

U.S. intelligence community's ability to identify these signals and help address the problem of lone-wolf terrorism. In short, this thesis asks, can the U.S. intelligence community harness the power of U.S. citizens through crowd-sourcing to help prevent lone-wolf terrorist attacks?

B. IMPORTANCE

Lone-wolf terrorism has emerged as a popular and effective tactic for terrorists attacking the United States. Eliminating the complex organizational framework inherent to a traditional terrorist group's structure makes it easier for lone-wolf terrorists to better avoid authorities' efforts to detect and prevent their violent acts. People seeking political change through violent acts is not a new phenomenon. With today's advances in science and vast amounts of information readily available to the masses through the Internet, individuals or smaller groups have the ability to cause massive amounts of destruction, a feat once reserved for much larger entities. Evidenced by such attacks as the Oklahoma City bombing, the DC sniper attacks, and the Boston Marathon bombing; this change in type and size of attack a lone actor is able to carry out has made lone-wolf terrorism a rising threat to society today.

The lone wolf presents particular challenges to the traditional U.S. intelligence community. Because a lone-wolf operator engages in, at most, minimal communication with a terrorist group hierarchy, the traditional intelligence procedures of identifying key members of a group are less effective. Also, using electronic intercepts to expand the search methods using a top-down approach is much less likely to identify and prevent terrorists using lone-wolf tactics.[3] Traditional SIGINT would identify the leader(s) of an organization and work to intercept communications. The lone wolf, however, rarely contacts a known terrorist group in a traceable manner, so he is more or less immune to SIGINT methods.

In today's Internet age, a lone wolf's interactions usually take the form of reading Internet forums and participating in, or simply observing, chat rooms dedicated to radical principals. As Tim Lister points out in his report, "Analysis of the backgrounds of dozens

[3] Ibid.

of young men who have embraced militant Islam and eventually planned or carried out an act of violence shows that. . . many become radicalized online."[4] Unless these individuals are already under investigation for unrelated reasons, there is little chance traditional methods of intelligence would discover such interactions. Many experts have advocated for a more thorough and pervasive information search by officials. Education of police on terrorism indicators, enhanced reporting procedures, engagement with community leaders, as well as general community outreach on the subject of terrorism have all been suggested.[5] But even these efforts are top-down in the sense that they are initiated, led by, and require large resource allocation by government officials.

There has been little, if any, research on, or advocating for, an approach different from this top-down method. Top-down methodology uses the resource intensive tools of extracting intelligence through an active network of agents and officials who are constantly canvassing and soliciting the population for information that would identify and predict terrorist activities.

Use of a grass-roots program such as crowdsourcing to gather intelligence on lone-wolf terrorists would reverse the information flow. This method has been proven effective in several relevant commercial applications such as the navigation application Waze, the human data processing endevour Mechanical Turk, and even the Defense Advanced Research Projects Agency's (DARPA) Ten Red Balloons experiment. In each of these examples, the information is pushed upwards rather than relying on the system to pull the information. Using local experts has vastly reduced the time to solve problems and increased information available to the whole system. Likewise, these same techniques of harnessing local experts—citizens—can be applied to the problem of

---

[4] Tim Lister, "How do we stop 'lone wolf' attacks?," *CNN*, October 27, 2014, http://www.cnn.com/2014/10/27/world/lone-wolves/.

[5] Michael P. Downing and Matt A. Mayer, "Preventing the Next 'Lone Wolf' Terrorist Attack Requires Stronger Federal–State–Local Capabilities," *Backgrounder*, no. 2818, June 18, 2013, http://www.heritage.org/research/reports/2013/06/preventing-the-next-lone-wolf-terrorist-attack-requires-stronger-federalstatelocal-capabilities.

Beau Barnes, "Confronting the One-Man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism," *Boston University Law Review,* vol. 92 (2012): 1631–40.

identifying lone-wolf terrorists with the same expected gains in information and decreases in time.

This new methodology has the potential to reduce the burden of information collection on the already overworked law enforcement cadre. It could also provide the U.S. citizenry with buy-in to the problem of terrorism prevention by making them active participants and thereby produce higher quality and larger amounts of intelligence than an unengaged community would. Additionally, using commercial innovations in crowdsourcing could streamline the information collection, processing, and distribution system to ensure the best data would be available in a timely manner to those organizations and personnel who could use it to prevent an attack.

Lone-wolf terrorism, its structure, its identifiers, and methods for detecting it have been thoroughly covered in previous literature. Additionally, much has been written on the grassroots method of crowdsourced solutions to various problems faced by modern society. But little work has been done to link these two issues. This thesis argues that a unique synthesis of this lone-wolf threat with crowdsourced solutions has the potential to revolutionize how the United States approaches terrorism prevention in the future.

C. PROBLEMS AND HYPOTHESES

Innovations in the commercial sector that rely on crowdsourcing to solve large and difficult problems provide a different roadmap towards a method for identifying lone-wolf terrorists before they strike. Crowdsourcing has proven useful, efficient, and fast in dealing with problems ranging from navigation, scientific research, photograph identification, and rapid geo-location of unique items and persons. The human mind is a better pattern identifier, context creator, and data relationship analyzer than any computer today.[6] It falls short in its speed and inability to process more than one item at a time. Crowdsourcing largely negates these shortfalls by establishing a parallel processing strategy for the participating human computers.

[6] Dominic Basulto, "Humans Are the World's Best Pattern-Recognition Machines, But for How Long?," *Big Think*, July 24, 2014, http://bigthink.com/endless-innovation/humans-are-the-worlds-best-pattern-recognition-machines-but-for-how-long.

Using these crowdsourced techniques in the domestic intelligence field should provide the same benefits that have been reaped in the commercial sectors. The Waze navigation application and Google Maps are both able to collect, analyze, and display traffic data received from thousands of participants in real time so that drivers are provided the most current traffic conditions and hazards on the road at the moment. *Wired Magazine* journalist Evan Ratliff attempted to disappear from public view for thirty days by going off the grid and relocating to a different city. A team using crowdsourcing techniques was able find him in 25 days.[7] Though the stakes are much higher, the identification of suspicious and potentially violent lone-wolf terrorists is no different procedurally from many of these tasks completed successfully by commercial crowdsourcing.

The key elements of these tasks are the large and distributed sources of information coupled with a method of quickly and easily collecting and interpreting the data in a manner that is useful to the participants. Indeed, several local attempts to enact this sort of program have been initiated by multiple cities and municipalities, including the Massachusetts Bay Transit Authority, the Atlanta Rapid Transit Authority, and most notably the New Jersey Office of Homeland Security and Preparedness.[8] Chapter II explains how they have all fallen short and produced insignificant information largely because they lacked the scale necessary for such an endeavor. With limited exposure and the resulting limited participation by citizens, these efforts provide little data for the systems to analyze.

In crowdsourcing, the larger and more visible problems, which capture public interest, typically result in wider participation by the populace. This wide participation is critical to the viability of crowdsourcing as a solution to a problem. With large amounts

---

[7] Christopher M. Ford, "Twitter, Facebook, and Ten Red Balloons: Social Network Problem Solving and Homeland Security," (master's thesis Naval Postgraduate School, 2011), 2.

[8] SAFE-NJ Itunes preview, Apple, accessed August 30, 2014, https://itunes.apple.com/us/app/safe-nj/id791702468?mt=8.

MARTA See & Say Itunes preview, Apple, accessed August 30, 2014, https://itunes.apple.com/us/app/marta-see-say/id620437590?mt=8.

MBTA See Say Itunes preview, Apple, accessed August 30, 2014, https://itunes.apple.com/us/app/mbta-see-say/id523210770?mt=8.

of data and inputs from a wide variety of sources, data can be statistically analyzed and trends discerned. Additionally, spurious data is more easily filtered out with large amounts of data to compare. With a small number of data points, statistical analysis and big data manipulation are problematic because each piece of data stands alone and there is much less ability for the pieces of data to overlap and reinforce that which is true and flag those pieces that are false.

In simple terms, crowdsourcing is much like determining the type of vehicle sitting in a parking lot based solely on the raindrops left on the ground from a storm. With only a few drops, the outline of the vehicle is indefinite and one may only be able to determine the very general class of it. As more raindrops strike the ground or are deflected by the vehicle, a more detailed and descriptive outline appears. Additionally, a few errant drops thrown under the vehicle from another passing vehicle could cause much more confusion to the analysis when there are only a few raindrops than when the outline was well established with many data points. As such, the most promising solution to identifying lone-wolf terrorists before they strike is a nationwide crowdsourced project that taps into the local expertise of the average citizen.

This thesis argues that a national crowdsourcing intelligence program would need to be well publicized and promoted to ensure sufficient participation by the populace. Additionally, it would need to be in a format that most people are comfortable and familiar with. Ease of use and minimization of participants' time and effort required for the program would be of high priority as well, based on current crowdsourcing doctrine. Gamification, "the use of game thinking and game mechanics in non-game contexts to engage users in solving problems,"[9] using intrinsic and virtual rewards, also will be important in order to maintain user participation and recruit new users to the program.

On the back end of the process, preliminary research indicates that a centralized database to collect all inputs, categorize them, and make them available for analysis will be critical for use by law enforcement officials. Connecting the dots is much more

[9] Sebastian Deterding, Dan Dixon, Rilla Khaled, and Lennart Nacke, "From Game Design Elements to Gamefulness: Defining 'Gamification'," in *Proceedings of the 15th International Academic MindTrek Conference*, 2011, 9–15, https://www.cs.auckland.ac.nz/courses/compsci747s2c/lectures/paul/definition-deterding.pdf.

effective when there are more dots to connect and a large central database is the best way to ensure the maximum amount of data is being cross-referenced and compared to one another. With wide dissemination to and adoption by the population, a centralized crowdsourced initiative has the capability of collecting large amounts of pertinent data on potential lone-wolf terrorism indicators identified by the local experts, the citizens.

D. METHOD AND OVERVIEW

This thesis uses a two-pronged approach, combining research on lone-wolf terrorist tactics and methodology with research into the use of crowdsourcing for solutions to problems deemed untenable using traditional methods. The thesis consists of five chapters, with Chapter I containing an introduction, the research question, an explanation of the study's relevance, problems and hypothesis, research method, literature review, and road map.

The lone-wolf terrorist problem is examined in Chapter II. It begins with several case studies of specific instances in which lone-wolf tactics were used by terrorists. They are profiled to identify indicators of potential lone-wolf actions. These case studies include the 1995 Oklahoma City Bombing by Timothy McVeigh; the 2010 attempted car bombing of an Oregon Christmas tree lighting by Mohamed Osman Mohamud; and the 2010 threatening of television producers and subsequent attempts to obtain foreign training to carry out attacks by Zachary Chesser. Case study analysis is the primary method used for the examination of lone-wolf tactics and to identify potential patterns of behavior that could detect terrorists using these tactics before they strike. The case study set includes both successfully executed lone-wolf attacks and ones which were foiled. Chapter II concludes with an examination of current methods of identifying and preventing lone-wolf terrorists that are being implemented by law enforcement agencies in the United States. It draws from both scholarly works on the subject as well as firsthand accounts published by law enforcement officials. It identifies deficiencies in the identification process inherent to both the current methods and proposed traditional solutions in publication.

Chapter III examines crowdsourcing as a general tool for solving problems and asks whether this solution would be applicable to the problem of detecting lone-wolf terrorists. It reviews current industry uses of crowdsourcing and identifies the methodology's strengths and weaknesses as well as which general types of problems crowdsourcing tends to excel at solving. It examines several case studies, to include; the navigation application Waze, the human data processing endevour Mechanical Turk (MTurk), and the Defense Advanced Research Projects Agency's (DARPA) Ten Red Balloons experiment. Through the analysis of these commercial efforts at crowdsourcing, the thesis attempts to identify the aspects of each program that made it successful at completing its assigned task and the advantages a crowdsourcing technique provides as well as the disadvantages involved. It is hypothesized that crowdsourcing excels at solving problems that are structurally similar in nature to the problem of identifying and predicting lone-wolf terrorist actions. Chapter III compares the types of problems that crowdsourcing has excelled at with the indictors of lone-wolf terrorism identified in Chapter II in order to confirm that crowdsourcing intelligence is feasible.

Chapter IV accounts for previous limited uses of crowdsourcing in the counterterrorist field and explains why these attempts have been largely unsuccessful. By examining these previous crowdsourcing methods, both successful commercial endeavors and the less successful counterterrorist applications, this chapter outlines a potential method of using crowdsourced intelligence successfully to identify and prevent lone-wolf terrorists. The thesis fuses the research conducted of lone-wolf attack case studies with the information obtained on crowdsourcing business problems. Doing so, it will attempt to merge a disparate problem set with solution options in order to discover a unique and effective answer to the important and growing problem of preventing lone-wolf terrorist attacks. An examination of the viability of using these crowdsourcing techniques in solving this identification problem will be conducted using a simple comparison of identified problems with possible solutions that crowdsourcing affords. The problems that have been solved using crowdsourcing techniques hold great promise for the prevention of lone-wolf terrorism because of the close similarities shared between them and the problem of identifying lone-wolf terrorists. Specifically, crowdsourcing has

proven itself at finding lone individuals or isolated items in record times and at collecting, processing, and condensing large amounts of data from disaggregate sources to provide a unified picture of the situation. Both of these are problem sets that are directly applicable to the search for and identification of terrorists using lone-wolf tactics. Chapter IV concludes with ancillary measures required to successfully implement a crowdsourced counterterrorism effort and some added non-counterterrorism benefits inherent to a crowdsourced approach to intelligence.

Chapter V provides a conclusion to the thesis and summarizes the findings of the previous chapters. It presents a addresses the counterargument against creating another form of domestic intelligence in light of the multitude of programs currently in existence. It also makes recommendations on how a crowdsourced domestic intelligence program could best be structured within current government institutions, as well as providing recommendations for further study on the subject.

E. LITERATURE REVIEW

This section begins by examining the academic works on the subject of organized Islamic terrorism in general and its evolution from hierarchical organization to one of lone-wolf tactics. It will then look at works on lone-wolf terrorism specifically in an effort to discern the indictors that precede attacks by lone-wolf terrorists. Once the literature on terrorism and lone-wolf terror tactics are examined, the review will shift its focus and look at academic works on the subject of crowdsourcing, searching for advantages, disadvantages, and potential similarities between the problems crowdsourcing has solved in the civilian sector and the problem of identifying lone-wolf terrorists.

1. Al-Qaeda: From Hierarchy to Lone Wolf

Al-Qaeda serves as an excellent case study for this thesis. It is a group whose evolution from hierarchical organization to franchise and finally to lone wolves has been extensively documented. While the present research question does not focus on combating traditional hierarchical groups, understanding their development, organization, and evolution are critical, as lone-wolf tactics often develop and evolve from hierarchical

organizations. Al-Qaeda itself is a constant, thus in comparing the group when it was a hierarchical organization to when lone-wolf tactics dominated, many of the variables, such as ideology and goals, are removed from the comparison of hierarchical terrorism to lone-wolf terrorism. This process brings into greater contrast the differences lone-wolf methodologies present from the more traditional hierarchical groups.

Examination of Al-Qaeda as a primary case study for a terrorist organization's formation, development, and eventual collapse can be examined using several excellent sources. For example, Peter Bergen's *The Osama bin Laden I Know: An Oral History of Al-Qaeda's Leader* contains firsthand accounts detailing the early life of Osama bin Laden, his motivations in resorting to terrorism, and his rise to prominence and the eventual leadership of Al-Qaeda.[10] Fawaz Gerges' *The Rise and Fall of Al-Qaeda* is another work that provides a historical perspective on Al-Qaeda's development.[11] Al-Qaeda was formed as a strictly hierarchical organization, but as pressure was applied and assets severed by opposing forces, Al-Qaeda was forced to evolve over time. This evolution took the form of local franchise groups initially and then evolved even further to an individual focus with lone-wolf tactics as its centerpiece.[12] Understanding why and how lone-wolf tactics developed sheds light on their methodology and provides insight into ways to identify and prevent attacks using these tactics. Gerges' last few chapters profile Al-Qaeda's fracturing under international pressure. The resulting shift in tactics and procedures to lone-wolf tactics is particularly illuminating and useful for this thesis.

There is a scholarly consensus that hierarchical terrorist organizations rarely choose lone-wolf tactics freely and of their own volition.[13] Often, terrorist organizations

---

[10] Peter Bergen, *The Osama bin Laden I Know: An Oral History of Al-Qaeda's Leader* (New York: Free Press, 2006).

[11] Fawaz Gerges, *The Rise and Fall of Al-Qaeda* (Oxford: Oxford University Press, 2011).

[12] Ibid., 110.

[13] Gerges, *Rise and Fall of Al-Qaeda*, 125, 152–154.

Bergen, *The Osama bin Laden I Know*, 385, 388, 393.

Christopher J. Fettweis, "Freedom Fighters and Zealots: Al-Qaeda in Historical Perspective," *Political Science Quarterly,* 124.2 (2009), http://www.psqonline.org/viewContent.cfm?sk=29F4EBCED6D60BF9C81DC9DB58C967B21ACDE1AFAE0DDBD3A087B2D1B09BE2CEEE, 288.

try to portray the shift to a "leaderless resistance" as a positive and empowering act, but it is usually a tactic to which they resort out of desperation once the hierarchical structure has become untenable due to disrupted lines of communication and an inability to maintain higher leadership in positions of control.[14] As such, lone-wolf terrorists are acting from a position of weakness and desperation rather than one of power. This position of weakness makes them no less deadly, but may provide insight into their motivations, thought processes, and methodologies—which will change based on this new position of weakness. These changes, such as reduced communications, more insular planning, and large increases in compartmentalization, result in indicators which are different and more subtle than those hierarchical terrorist organizations emit and which traditional intelligence collection methods have concentrated on in recent past. As such, a different method of detecting these new and subtle indicators is needed.

2. Lone-Wolf Terrorism: A Unique Threat

Literature on lone-wolf terrorism specifically has blossomed in the past decade as Al-Qaeda began to use lone-wolf tactics to a much greater extent. Scholars have completed comprehensive case studies of terrorist attacks using lone-wolf tactics and have examined not just what lone-wolf terrorists are, but also how they operate, as well as indicators and preparations for persons using these tactics. Raffaello Pantucci's *A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists* serves as an academic touchstone in defining what a lone-wolf terrorist is and what sort of tactics are typically involved. Pantucci states in his opening paragraphs that, "The term Lone Wolf terrorist in this article is used to refer to individuals pursuing Islamist terrorist goals alone, either driven by personal reasons or their belief that they are part of an ideological group."[15] This thesis draws largely from his definition of who can be categorized as a

---

[14] Scott Stewart, "Cutting Through the Lone-Wolf Hype," *Security Weekly*, September 22, 2011, https://www.stratfor.com/weekly/20110921-cutting-through-lone-wolf-hype.

Matthew Cole, "Al-Qaeda Promises U.S. Death By A Thousand Cuts," *ABC News*, November 21, 2010, http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726.

[15] Raffaello Pantucci, "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists," *Developments in Radicalisation and Political Violence*, March 2011, 9, http://icsr.info/wp-content/uploads/2012/10/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf.

lone wolf when establishing the set of attacks, actors, and surrounding events that will be analyzed, broadening the lens beyond Islamist terrorist goals to terrorist goals writ large.

One of the most useful aspects of Pantucci's definition is the broad net that can be cast with it. In fact, the sentence that follows his definition of a lone-wolf terrorist states, "The term Lone Wolf is expanded out to Lone Wolf pack when referring to small isolated groups pursuing the goal of Islamist terrorism together under the same ideology, but without the sort of external direction from, or formal connection with, an organized group or network."[16] This thesis differs from his specific definition only in opening it up to other ideologies than radical Islamists. It is well established that radical Islamists neither invented nor hold a monopoly on the use of lone-wolf tactics. As such, Pantucci's definition is too narrow in this respect. Using a modified form of his definition, events that are traditionally considered lone-wolf attacks—for example, Timothy McVeigh's bombing of the Oklahoma City federal building—can be included even though several accomplices were discovered; thus, it was not, strictly speaking, an attack by an isolated actor. While events such as the Oklahoma City bombing and the Times Square bombing differ in ideology, the reasons for using lone-wolf tactics and the methodologies used by both attackers to prepare are similar. This indicates that methods of detecting one lone-wolf terrorist may be applied to all lone-wolf terrorists, regardless of ideology.

Ramón Spaaij's "The Enigma of Lone Wolf Terrorism: An Assessment" takes a much narrower view of lone-wolf terrorism and maintains that only those individuals operating completely alone and with no outside help can be considered lone wolves.[17] The 2012 Aurora, Colorado shooting is a prototypical example that complies with Spaaij's definition of a lone-wolf terrorist since James Holmes planned and executed the entire event without any support from other parties. Despite this more restrictive definition of lone-wolf terrorism, the other portions of Spaaij's work provide many useful insights into lone-wolf terrorists' actions. Specifically, it examines the motivational patterns of lone-wolf terrorists, the social and psychological circumstances that motivate

---

[16] Ibid., 9.

[17] Ramón Spaaij, "The Enigma of Lone Wolf Terrorism: An Assessment," *Studies in Conflict & Terrorism* vol. 33, no. 9 (2010): 856.

individuals to engage in lone-wolf terrorism, and the links between lone-wolf terrorists and other terrorist subjects, networks, and ideologies.[18] These insights are useful not only in examining what type of person has conducted lone-wolf terrorist attacks already, but also what type of people are more likely to use this method in the future. If these indicators of lone-wolf terrorism preparation and planning can be codified, even if they are as subtle as they are expected to be, then that framework can be used to analyze intelligence data and thereby better prevent lone-wolf terrorist attacks.

Beau Barnes' "Confronting the One-Man Wolf Pack" picks up where the other titles leave off.[19] He begins by briefly outlining the origins and definition of lone-wolf terrorism and then proceeds to identify methods currently in use by law enforcement to predict and prevent lone-wolf tactics. He describes the current process as a top-down approach that attempts to penetrate society itself in order to pull out pertinent information concerning terrorism. He continues with a discussion on why these measures fall short and have been so unsuccessful in preventing lone-wolf tactics in the recent past. Traditional electronic surveillance provides much larger amounts of data than can be processed at a central location, analyzing every Tweet, Facebook post, and e-mail sent is too large a task. This fire hose of data can only be managed effectively when it is narrowly focused on an already identified target of interest and does poorly at wide canvassing for initial indicators.

This limitation has been recognized by law enforcement officials and has spawned alternative methods of wide-area canvassing for counterterrorism intelligence such as community outreach. Community outreach suffers its own limitations with an exponentially increasing workload on the collector as the intelligence coverage is increased. A single police officer can only interact with a finite number of local citizens in order to gather domestic intelligence and there are more people to contact than there are police officers available to do so. As such, several solutions are available: one can accept the resource limitations and only reach out to a portion of the citizenry, one can increase law enforcement budgets to support larger numbers of officer to conduct

[18] Ibid., 855.

[19] Barnes, "Confronting the One-Man Wolf Pack," 1620-1621.

community outreach, or one can empower the citizens themselves to push the intelligence they have, as local experts, up to the appropriate officials. This third alternative has the potential of increasing intelligence collected without the proportional increases in law enforcement resources expended. It also may empower the citizenry by making them part of the solution and thereby generate better quality and larger volumes of intelligence. Ultimately, Barnes echoes many other sources in the belief that lone-wolf tactics pose a separate and unique problem to intelligence and law enforcement officials and further states that those agencies' traditional methods of identification and prevention are ill-suited to this problem.[20]

Alex Shone's work serves as an important primer for further consideration of those topics already discussed in this section as well as highlighting how law enforcement efforts should change in order to adapt to the unique threat of lone-wolf terrorism. Shone maintains in his article that:

> Counterterrorism services need to be far more attuned to those signals, as minimal as they might be, that any individual with a terrorist intent will inevitably give off in preparing his attack. This requires not only effective data capture and exploitation enabled by efficient overall information management, but also fused intelligence products. This requires intelligence analysts and collectors to work in far closer union.[21]

This statement is echoed in several other academic works in the lone-wolf terrorism field and provides a useful segue into determining the best methods for law enforcement officials to use to identify and prevent lone-wolf terrorist before they attack. His further general insights into this topic make it apparent that using current technologies to crowdsource this problem could serve as a viable part of the solution.

3. Crowdsourcing Intelligence: A Possible Alternative

Unlike the topic of terrorism or even lone-wolf terrorism, crowdsourcing is a relatively new field with less academic discourse on the topic. The term itself only came

---

[20] Ibid., 1650–53.

[21] Alex Shone, "Countering lone wolf terrorism: sustaining the CONTEST vision," *The Henry Jackson Society*, May 17, 2010, http://henryjacksonsociety.org/2010/05/17/countering-lone-wolf-terrorism-sustaining-the-contest-vision/.

into existence in 2006 when it was coined by Jeff Howe in a *Wired Magazine* article on the subject.[22] An examination of the literature that is available on the subject is crucial though, since initial analysis shows crowdsourcing as a promising technique for identifying lone-wolf terrorists before they strike. Jeff Howe, in *Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business*[23], provides many useful insights into crowdsourcing, the basis for its approach, ways to maximize its effectiveness, and why it has come of age so recently. A key point found throughout his book is that the most successful crowdsourcing initiatives have had top-down guidance but bottom-up participation with an emphasis on community building. According to Howe, "What unites all successful crowdsourcing efforts is a deep commitment to the community."[24] This may be the most difficult paradigm shift that the intelligence community will need to tackle in order to make crowdsourcing a viable method of domestic intelligence collection since it runs counter to many of the well-ingrained practices and procedures of the field. If successful, crowdsourcing has the potential to provide the intelligence community with many benefits, both direct and indirect. Direct benefits such as increased insight into communities and more intelligence sources for potential threats are obvious. Indirect benefits such as citizen buy-in to the problem of counterterrorism and better public relations due to increased transparency and participation might be less obvious and will warrant further investigation.

Daren Brabham, in a preeminent work, succinctly defines crowdsourcing as, "an online, distributed problem-solving and production model that leverages the collective intelligence of online communities to serve specific organizational goals."[25] This definition is not only representative of what crowdsourcing means to most scholars in the field but it provides a broad enough framework to enable the inclusion of government as well as private uses. Most importantly for this thesis, Brabham further outlines general

---

[22] Jeff Howe, "The Rise of Crowdsourcing," *Wired Magazine*, June 2006, http://archive.wired.com/wired/archive/14.06/crowds.html.

[23] Jeff Howe, *Crowdsourcing: Why the Power of the Crowd is Driving the Future of Business* (New York: Three Rivers Press, 2008).

[24] Howe, *Crowdsourcing*, 15.

[25] Daren Brabham, *Crowdsourcing* (Cambridge, MA: MIT Press, 2013).

types of problems or tasks at which crowdsourcing excels and those tasks at which crowdsourcing is less useful than other currently available methods of problem-solving. Crowdsourcing has two sides: the front end of gathering data from distributed human sources and the back end of compiling and analyzing this data in a manner that makes the results useful for the end-user. Thus, crowdsourcing can be equated to the intelligence process of collection and analysis, and in much the same way; one cannot be effective without the other. As such, research into the back end data analysis of crowdsourcing is as important as the front end in evaluating its uses in countering the lone-wolf threat.

James Manyika and Michael Chui's *Big Data: The Next Frontier for Innovation, Competition, and Productivity* is an examination of big data in the private sector and the effects that its use by businesses and industry have on their operation.[26] It outlines methods useful for maximizing big data's utility, such as increased transparancy and support of human decision making with automated algorithms.[27] It also highlights such pitfalls as not having people with requisite statistical and analytical skills staffed in an organization to deal with big data.[28] This thesis uses this work in order to outline the requirements for the operator's side of any crowdsourced solution to lone-wolf identification.

Crowdsourcing has proven itself at finding individuals or isolated items in record times and at collecting, processing, and condensing large amounts of data from disaggregate sources to provide a unified picture of the situation. Both of these are problem sets that are directly applicable to the search for and identification of terrorists using lone-wolf tactics. *Twitter, Facebook, and Ten Red Balloons Social Network Problem Solving and Homeland Security* by Christopher Ford and *Inflated Expectations: Crowd-Sourcing Comes of Age in the DARPA Network Challenge* by Larry Greenemeier both examine the most famous crowdsourcing case to date, namely, DARPA's Ten Red Balloons experiment. In this experiment, DARPA sponsored a contest to locate ten

---

[26] James Manyika and Michael Chui, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (Washington, DC: McKinsey Global Institute, 2011).

[27] Ibid., 97–99.

[28] Ibid., 103–104.

tethered red balloons scattered throughout the continental United States at unknown locations. The goal was for an individual or team to locate all ten balloons and report their locations. DARPA estimated one week as the time required to complete the task. Using a dispersed network and crowdsourcing techniques, the winning team located all ten balloons in less than nine hours. Of specific importance to this thesis, both Ford and Greenemeier discuss the team's methods of validating and confirming reported sightings despite a deluge of false reports generated by other teams. This is a prime example of the use of crowdsourcing and big data manipulation to solve a real-world problem and provides excellent precedent for application of the same techniques in counterterrorism.

Chris Nodder's *Evil by Design: Interaction Design to Lead Us into Temptation* is an excellent source for several other examples of crowdsourcing solutions to commercial problems, which include the navigation application Waze, the cellular biology research project Foldit, and the coupon selling program Groupon.[29] Examination of these cases as well as the reasons behind each of their success will provide guidance on what a crowdsourced solution to identifying lone-wolf terrorists should incorporate in general terms. There are several other works on the subject of crowdsourcing which provide further examples of its use. These examples include not only commercial endevours but also government attempts to harness the power of the masses to solve problems such as combatting organized crime, responding to crisis events, and protecting public safety. In each one, the method of employment is detailed as well as any success or setbacks encountered in the process. Of more specific utility are the discussions on how to limit the influence of spurious data,whether it be intentional or unintentional in nature. This is a major problem forseen with crowdsourcing domestic intelligence and insights into methods of preventing spurious data are especially useful to this thesis.

Though sparse, a few attempts at crowdsourcing problems related to homeland security and terrorism prevention specifically have been made. One attempt, funded by the Intelligence Advanced Research Projects Activity (IARPA), uses a market-based approach to the crowdsourcing of the intelligence community's knowledge by asking

[29] Chris Nodder, *Evil by Design: Interaction Design to Lead Us into Temptation* (Indianapolis, IN: John Wiley & Sons Inc., 2013), 211–215.

experts to make predictions about potential global events such as the progress of the Free Syrian Army or if Kim Jong Un will resign as leader of North Korea.[30] This project has been put on hold several times due to backlash and resentment from the traditional intelligence community but has been proven to be quite accurate in predicting certain outcomes of such large-scale events. For example, "Intrade's consensus called every state correctly in the 2004 U.S. presidential election and all but two right in 2008."[31] Some of the backlash may be understandable and related to poor timing since the original IARPA effort involved placing odds on the next large terrorist attack and it was launched months before the 9/11 tragedy. Other, more general, critiques—such as former senior CIA and State Department analyst Mark Lowenthal's statement that, "I don't believe in the wisdom of crowds. Crowds produce riots. Experts produce wisdom."[32]—may be relics of outdated thinking based on old paradigms. The same argument Lowenthal expresses has been made in the private sector but has been disproven both scientifically and through real-world experience multiple times.[33] While not exactly in line with identifying lone-wolf operators, the problems of public perception and professional acceptance faced by this project and the methods for overcoming those problems are relevant in solving similar problems encountered in crowdsourcing the identification of lone-wolf terrorists.

Likewise, an article in *Intelligence and National Security* titled, "Introducing Social Media Intelligence (SOCMINT)," provides parallel examples of large data collection and using crowds to gather intelligence in order to combat crime and terrorism.[34] Though more focused on pulling data from social media rather than have it voluntarily pushed up by the citizens, this article also touches on user participation in the collection, lending a crowdsourced aspect to the process. The most salient points in this

---

[30] Ken Dilanian, "America's Top Spies Go Up Against a Crowd," *Los Angeles Times*, August 21, 2012, http://articles.latimes.com/2012/aug/21/nation/la-na-cia-crowds-20120821.

[31] Ibid.

[32] Ibid.

[33] Brabham, *Crowdsourcing*, 20–21.

Howe, *Crowdsourcing*, 11.

[34] David Omand , Jamie Bartlett, and Carl Miller, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security*, 27:6, 801–823, http://www.academia.edu/1990345/Introducing_Social_Media_Intelligence_SOCMINT_.

SOCMINT article are the discussions on backend compilation and discrimination of data for such an endeavor, as well as the discussion on the public relations campaign which must be successfully executed to ensure the viability of such a program as SOCMINT or crowdsourced intelligence. This need for public buy-in to the process is rarely discussed in the intelligence literature as a whole and therefore makes this article even more valuable.

Crowdsourcing of domestic intelligence provides another important advantage over traditional top-down intelligence collection methods. By making the program voluntary with cooperative participation by the citizenry, 4th Amendment issues of privacy and civil liberties are largely nullified. This is because, at its essence, crowdsourcing is no different than police crime hotlines which have been used for decades with no issue. The 1983 Supreme Court case *Illinois v. Gates*, 462 U.S. 213 sets precedent for such anonymous tips and how they may be used by law enforcement to begin their own investigations.[35] Crowdsourcing using mobile applications or other technological methods only has the potential to differ in volume of information passed and ability of law enforcement to utilize said data in a more efficient manner.

Ample research and academic literature is available for both of the two main points of this thesis, framing the problem of identifying lone-wolf terrorists and crowdsourcing solutions to large problems. Managing big data will also play a part in forming the solution and literature on that subject is as prolific, if not more so, than either of the other topics. There exists a gap in both academic and professional literature concerning the application of crowdsourcing methodology to the problem of identifying lone-wolf terrorists before they strike. While some literature has analyzed crowdsourcing for general homeland security needs, none found so far directly addresses the identification of lone-wolf terrorists. This thesis will fill the gap by applying the tested and proven crowdsourced solutions, which have been pioneered by the civilian sector, to the problem of identifying lone-wolf terrorists before they strike.

[35] U.S. Supreme Court, Illinois v. Gates, 462 U.S. 213, 1983 (Washington, DC, 1983), https://supreme.justia.com/cases/federal/us/462/213/case.html.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE LONE-WOLF PROBLEM AND CURRENT METHODS TO COMBAT IT

This chapter examines the lone-wolf terrorist problem. It begins with a historical account of the evolution of Al-Qaeda from one of the world's most powerful and most hierarchical terrorist organizations to its current reduced standing and associated promotion of lone-wolf tactics. By comparing hierarchical Al-Qaeda with dispersed Al-Qaeda, it establishes the reasons individuals gravitate to lone-wolf tactics as well as the advantages and disadvantages inherent to those tactics. Based on those advantages and disadvantages, the difficulties faced by law enforcement and intelligence services in detecting lone-wolf operators are laid out. Next, several case studies in which lone-wolf tactics were used by terrorists are shown in an effort to identify early indicators of potential lone-wolf actions. Chapter II concludes with an examination of current methods of identifying and preventing lone-wolf terrorists that are being implemented by law enforcement agencies in the United States. It identifies deficiencies in the identification process inherent to both the current methods and proposed traditional solutions in publication. The purpose of Chapter II is to highlight the gaps in the traditional domestic intelligence system and explain how lone-wolf terrorists are specially poised to fall into those gaps and evade detection.

A. AL-QAEDA: FROM HIERARCHY TO INDIVIDUAL

Al-Qaeda, formed by Osama bin Laden during the splintering of al-Tanzim al-Sirri in 1966, was the antithesis of its parent organization.[36] Whereas al-Tanzim al-Sirri was a grassroots effort with very local concerns and objectives that looked inward to the Muslim world, Al-Qaeda was an extremely hierarchical entity with tight controls administered by Bin Laden, and one that espoused large goals such as attacks on enemies of Islam and their *jihad*, or holy struggle, in foreign lands such as Israel and other previously Muslim countries. Al-Qaeda spent several decades in the development stage

[36] Bergen, *The Osama bin Laden I Know*, 80–81.

Gerges, *Rise and Fall of Al-Qaeda*, 30.

but by the late 1980s, it was an organized and effective terrorist group with significant striking power and considerable reach. By the mid-1990s, Al-Qaeda had established its base of power in Afghanistan under a Taliban sanctuary and Osama Bin Laden began issuing *fatwas*, religious edicts, which called for a global jihad and declared war on the United States and its allies.[37]

Seen as the height of Al-Qaeda's hierarchical reign, these bold steps garnered international attention and enabled Al-Qaeda to recruit combat veterans from Bosnia, Algeria, Egypt, Iraq, and elsewhere. These veterans brought expertise and planning with them that enabled such attacks as the 1993 World Trade Center bombing and the attack on the *USS Cole* (DDG 67). Al-Qaeda's support base and operational range continued to grow through the following years and culminated in one of the boldest asymmetric attacks in history, the September 11th attack on the United States. Both a boon and a curse to Al-Qaeda, the attack would thereafter define Al-Qaeda as a whole and Bin Laden in particular. It served as a recruitment beacon to their cause for new fighters but also drew the ire of the entire civilized world, including most of the Muslim world. The event was polarizing and while it mobilized the most extreme and militant of jihadists, it also turned Al-Qaeda into a pariah which few other groups, Muslim or otherwise, wanted to touch.[38]

After the fall of the Taliban to the U.S. military, Al-Qaeda was splintered and Bin Laden was forced to seek sanctuary in Pakistan. From there, he was able to establish a resistance to the U.S. occupation of Iraq and Afghanistan but saw the size of his forces reduced dramatically as country after country complied with U.S. efforts in eliminating or capturing Al-Qaeda operatives. This pressure on the central hierarchy led to the development of franchises of Al-Qaeda in specific geographic areas such as Al-Qaeda in Iraq (AQI) and Al-Qaeda in the Arabian Peninsula (AQAP). This franchising brought some much needed flexibility and redundancy to the very hierarchical command structure

---

[37] Osama Bin Laden, "Text of Fatwah Urging Jihad Against Americans," *Al-Quds al-'Arabi*, February 23, 1998, http://web.archive.org/web/20060422210853/http://www.ict.org.il/articles/fatwah.htm.

[38] Gerges, *Rise and Fall of Al-Qaeda*, 95, 103.

of Al-Qaeda but had the negative effect of divesting Bin Laden of much of the detailed control he was used to.[39]

As sentiment turned against Al-Qaeda, it was forced to adopt a new structure which would be even less hierarchical than the franchise system. Al-Qaeda began issuing statements which rallied individual jihadists to action at the lowest level and with minimal contact with its command structure. Embracing a "strategy of a thousand cuts," Al-Qaeda hoped it could bleed the West dry by forcing it to spend billions of dollars to prevent attacks which only cost thousands of dollars to carry out.[40]

B. EMERGENCE OF THE LONE WOLF

Today, Al-Qaeda is more an ideological basis for radicals than a military organization. Splinter groups still exist throughout the Middle East but are poorly manned and are rarely welcomed by host countries fearful of U.S. involvement and reprisals. Instead, its teachings and philosophy stand as a beacon for disenfranchised individual Muslims who want to take on the jihadist mantle and strike a blow against the godless West. As Gerges states, "Al-Qaeda's ideology sanctions the killing of the enemies of Islam, including civilians, and therefore adapts easily to different temperaments, backgrounds, and concepts of victimhood. Al-Qaeda's top-down recruitment of would-be terrorists has been, for the most part, replaced by a bottom-up process, a product of rising tensions and hostilities."[41] In his conclusion, Gerges provides insight into why these self-motivated bottom-up recruits are taking up the jihad by explaining that:

> Bottom-up radicalization has less to do with al-Qaeda Central and more with the side effects of the raging War on Terror in the greater Middle East. I interviewed several homegrown suspects who were found guilty in U.S. courts and almost all of them specifically mentioned the conflicts in Iraq, Afghanistan, and Pakistan as the main cause for their radicalization; of course they railed against the U.S. War on Terror, which they viewed as

[39] Ibid., 95, 110.

[40] Cole, "Al Qaeda Promises U.S. Death."

[41] Gerges, *Rise and Fall of Al-Qaeda*, 152.

> a crusade against Islam and Muslims, but identity politics was the real driver behind their migration to militancy.[42]

He further expounds that these self-radicalized jihadists were not necessarily fighting for the Al-Qaeda cause but were fighting against the injustices they viewed the United States and the West perpetrating against the Muslim community as a whole. Al-Qaeda simply served as a convenient touchstone for them and an easy way to legitimize their own individual grievances and their violent means of addressing those grievances.[43]

In many ways, this evolution of Al-Qaeda from hierarchy to lone wolf can be seen as a rudimentary form of crowdsourcing itself. By endorsing lone-wolf tactics and encouraging its use by Al-Qaeda's base of support, it is fulfilling two of the three major requirements of a crowdsourcing endeavor: top-down guidance for overarching goals with bottom-up participation and development of the procedure. The one missing aspect, community building, is necessarily excluded since two-way communications and the establishment of dialogues would open the process up to traditional intelligence collection by Al-Qaeda's enemies. Instead, by keeping the communication a broadcast rather than dialogue, this fractured and reduced organization of Al-Qaeda is able to continue to exert its influence and lay claim to many more, albeit smaller, acts of terror than it could have using traditional hierarchal methods. It is this desire to continue to exert a global influence even with a greatly reduced cadre of leaders and soldiers that has driven Al-Qaeda to outsource its terrorist operations to the masses. To a certain extent, U.S. actions against Al-Qaeda over the past decade and the resulting collateral damage and unintended consequences have facilitated this outsourcing by developing a base of disenfranchised and angry young Muslims who oppose U.S. behavior and are open to Al-Qaeda's message of individual jihad. Al-Qaeda can then tap this pool to act as independent agents of terror.

As has been alluded to previously, there are some definite advantages for an organization that adopts or endorses lone-wolf tactics. Stated simply, low cost and difficulty in preventing the attacks are the two primary advantages that lone-wolf tactics

---

[42] Ibid., 160.

[43] Ibid., 161–164.

have over other forms of terrorism. From a terrorist group's point of view, stoking the flames of hatred within individuals that have an inherent grudge against similar enemies and endorsing violence against those targets is much less expensive than carrying out the attack itself. Lone-wolf tactics negate the monetary and time investments terrorist groups have traditionally allocated to training operatives, planning an attack, and outfitting the operatives with the resources they needed to carry out the attack.

Recent technology such as the Internet and e-mail has made the costs associated with indoctrinating lone-wolf operatives considerably cheaper. Books, writings, and manifestos were the norm for recruiting independent terrorists prior to the Internet revolution. These low-tech methods severely limited the number of potential lone wolves that could be reached.[44] With the Internet, groups can put their message out for worldwide consumption for just pennies a day in server hosting costs and can interact on a personal basis with anyone in the world with a computer and e-mail account. Cheap communication works to the advantage of the individual's being radicalized as well. With free access to any information on the Internet the cost of entry for a potential lone wolf is lowered. Previously, an individual would need to invest time and money in either buying a book or attending a speech. Now, all the same information can be attained from the convenience of their home using the Internet, a resource that most people are already purchasing for other reasons.

There is an added advantage of having such interactions be very discrete, which is closely linked with the same aspects of lone-wolf recruitment that make it cheap. Even in the past, an individual buying a book or attending a speech was unlikely to be noticed by officials in the United States or most other western countries. Now, with the anonymity of the Internet, disenfranchised and mentally disturbed individuals are free to scour any and all sites and articles which reinforce their burgeoning beliefs. They are able to anonymously interact with others who share their same point of view through anonymous chat rooms in which pseudonyms are the norm. This limited and anonymous interaction with terrorist groups, even ones on official watch lists, means that a potential lone wolf

[44] Rodger A. Bates, "Dancing with Wolves: Today's Lone Wolf Terrorists," *The Journal of Public and Professional Sociology*, vol. 4, no. 1 (2012): 4.

can attain guidance and technical assistance with a small likelihood of detection. The head of counterterrorism for the New York Police Department John Miller has stated, "If the conspiracy to commit a terrorist act is a conspiracy of one, and the planning for that is unsophisticated, doesn't require a lot pre-operational surveillance and is only happening in the mind of the offender, from an intelligence standpoint, from a prevention standpoint, that's very hard to detect."[45] This is a sentiment echoed countless times by both professional law enforcement and academics studying the issue. Anonymity works in the other direction as well. Using the anonymity of Internet communication allows Al-Qaeda to continue the fight against the West while the leadership remains in the relative safety of exile.

The final major advantage lone wolves typically have is their inherent knowledge of local customs, practices, and operating environment of their targets and surrounding areas. Though academic literature agrees that profiling a typical lone-wolf terrorist is impossible since they have a myriad of motivations which often mixes a terrorist group's rhetoric with their own personal grievances, one of the few trends readily documented is the tendency for lone-wolf terrorists to strike locally.[46] This local knowledge not only gives them the ability to better choose targets for their vulnerability and importance but also allows them to blend in and conceal their preparations from law enforcement officials.

One major disadvantage of lone-wolf tactics is the inherent lack of control terrorist groups can exert over operations. While they can recommend and present ideas and motivations, a group who has turned over activities to the crowd no longer has the degree of control a group using traditional command and control can exert. Al-Qaeda experienced this sort of hardship when their franchise in Iraq, under the leadership of Abu Musab al-Zarqawi, began targeting Sunni Muslims and as a result, alienated a large

---

[45] Tom Hays, "Lone-Wolf Terror Threat Focus of NYPD Conference," *ABC News*, November 6, 2014, http://abcnews.go.com/U.S./wireStory/lone-wolf-terror-threat-focus-nypd-conference-26746906.

[46] Michael Becker, "Explaining Lone Wolf Target Selection in the United States," *Studies in Conflict & Terrorism*, vol. 37,no. 11 (2014): 967–969.

Sarah Teich, "Trends and Developments in Lone Wolf Terrorism in the Western World: An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists," *International Institute for Counter-Terrorism*, http://www.ctcitraining.org/docs/LoneWolf_SarahTeich2013.pdf, 22.

portion of their support base. Al-Zarqawi was able to deviate from Bin Laden's orders to such a great degree because he had been given wide latitude in organizing and running AQI. This sort of issue is greatly exacerbated by the much looser ties that lone wolves have with their parent organizations.

Another disadvantage of lone-wolf tactics for terrorist organizations is the diffusion of their message, which can occur when such tactics are used. This can be equated to the problem of making a copy of a copy: an original image copied enough times becomes distorted to the point of being unrecognizable. Likewise, if a lone wolf is motivated by Al-Qaeda's original message but modifies it to fit his own world view and then successfully carries out an attack which might not strictly be in line with Al-Qaeda's message and purpose, this poses a copy issue. Long term, another disenfranchised individual may see that first lone wolf as inspiration for his own acts which deviate even further from Al-Qaeda's goals. This has been seen firsthand by Gerges, "Young activists in France, Spain, Britain, and Italy [are] out of touch with recent developments in Afghanistan and Pakistan."[47] This inability to firmly control and guide the group's message represents a long-term strategic disadvantage. In fact, the loss of control over terrorist acts as described previously is also a strategic loss. Both these long-term strategic losses are accepted by Al-Qaeda in exchange for the short-term tactical advantages that lone-wolf tactics bring; specifically, greater economy of force and increased secrecy of operations.

While lone-wolf tactics have their tradeoffs, their unique advantages are causing traditional intelligence collection methods to be rendered mostly impotent in the identification and prevention of terrorist attacks.[48] The U.S. intelligence community excels at its technical means of collection. Tapping phones, listening to satellite communications, and penetrating enemy computer systems are the hallmarks of U.S. intelligence efforts. For the most part, this emphasis on the technical has served the United States well, since it has coincided with the emergence and global domination of

[47] Gerges, *Rise and Fall of Al-Qaeda*, 165.

[48] Edwin Bakker and Beatrice de Graaf, "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed," *Perspectives On Terrorism* vol. 5, no. 5–6 (December 2011), http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf/334, 46.

the technology revolution. If all the enemy's secrets are digital, then that is where intelligence should focus its efforts. The lone wolf is largely protected from this method of collection though.[49] If there are no conversations then none can be intercepted. If the content of radical websites is freely known to all then the intelligence community may be able to obtain that information but has great difficulty ascertaining who else obtains it as well. With no direct hierarchical command structure, less technical means of collection such as human intelligence (HUMINT) are put at a large disadvantage as well.[50] Overall, this lack of command structure and limited communication means that lone-wolf terrorists are truly insulated from most traditional methods of intelligence collection and if the United States hopes to detect and prevent such attacks in the future, non-traditional means will need to be employed.

C. CASE STUDIES OF LONE WOLVES

Both Becker and Teich, in their works cited earlier, have compiled comprehensive databases of lone-wolf attacks upon U.S. soil over the past several decades and have been able to extrapolate some useful trends associated with lone-wolf terrorists as well as dispelling some commonly held, but incorrect, assumptions. Below are a selection of case studies which highlight the findings of those two comprehensive studies. These case studies call attention to the advantages lone-wolf terrorists possess, the challenges posed to traditional intelligence methods of identification, and potential means of detecting these lone-wolf terrorists.

Timothy McVeigh, the perpetrator of one of the deadliest terrorist attacks against the United States, serves as a good first example of a lone wolf because his development, radicalization, and methodology are so consistent with what experts have found to be a typical lone-wolf terrorist. McVeigh, a loner since childhood, due in large part to disinterested and inattentive parents and a trend of being bullied by peers, sought a sense of belonging from multiple different sources but maintained a loner's lifestyle. This

[49] Barnes, "Confronting the One-Man Wolf Pack," 1637–1638.

[50] Erik J. Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 168–169.

isolation developed to the point of purchasing land in New York for a survivalist bunker and eschewing traditional romantic pursuits.[51] While enlisted in the Army, one of the places McVeigh came closest to developing a social aspect, he continued the disturbing trend of extreme self-sufficiency and survivalist preparation. This was taken to the point that he "rented a storage shed in nearby Junction City, and just as he had done at his father's home back in Pendleton, he kept one hundred gallons of fresh water there, along with guns, ammunition, MRE rations, and other supplies."[52]

Disenchanted with life in the Army after failing to qualify for the Special Forces, McVeigh left the military and returned home to a dead-end job and became enraged at the system for failing him. During this time, he began to write anti-government letters to local newspapers.[53] Additionally, McVeigh became immersed in the gun show culture and recruited old Army buddies Terry Nichols and Michael Fortier to help sell items at these shows as a side business. During these years, McVeigh became more disillusioned with the federal government over their handling of the Ruby Ridge and Waco incidents and felt that U.S. citizens were oblivious to the inevitable restrictions on their rights. McVeigh came to trust Nichols and Fortier and eventually hatched a plan to bomb the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma in order to combat the federal government. McVeigh and his accomplices bought or stole the components for the bomb, and traveled great distances to acquire them. Paranoid of being discovered, McVeigh wrote to family members about his concerns of being surveilled by 'G-men'.[54] After assembling the bomb in Geary Lake, Kansas, McVeigh drove it to the Federal Building in Oklahoma City and detonated it from a distance.

Mohamed Osman Mohamud, a 19-year-old Somali-American man who plotted in 2010 to blow up a car bomb at an Oregon Christmas tree lighting ceremony in Portland

---

[51] Dale Russakoff and Serge Kovaleski, "An Ordinary Boy's Extraordinary Rage; After a Long Search for Order, Timothy McVeigh Finally Found a World He Could Fit Into," *The Washington Post*, July 2, 1995, A1.

[52] Lou Michel and Dan Herbeck, *American Terrorist* (New York: HarperCollins Publishers, 2001), 70.

[53] Michel and Herbeck, *American Terrorist*, 118.

[54] Brandon Stickney, *All-American Monster: The Unauthorized Biography of Timothy McVeigh* (New York: Prometheus Books, 1996), 65.

serves as another typical example of a lone-wolf perpetrator. An 18 year old college student with separated parents, Mohamud lacked many friends growing up and, in high school, reached out to the extremist jihad community in an effort to belong to a larger cause. He originally wrote physical fitness articles for the extremist magazine *Jihad Recollections* but quickly expressed a desire to be more directly involved with the cause.[55] FBI officials were "tipped from someone concerned about him"[56] and intercepted an e-mail exchange between Mohamud and a known terrorist recruiter living in Pakistan. After repeated failed attempts by Mohamud to contact a third party for assistance in traveling to Pakistan, the FBI spoofed the third party's e-mail address and contacted Mohamud. Recording all their interactions, the FBI provides much evidence of Mohamud's disengagement from society and his path towards terrorism.[57] An individual who wanted to take a stand and be part of something larger than himself, Mohamud attempted to detonate a car bomb which would have killed and injured hundreds of people had the FBI not intervened.

Zachary Chesser, an intelligent and successful student in Fairfax, Virginia, confessed to, and was found guilty of, aiding the terrorist organization Al-Shabaab.[58] The child of divorced parents, Chesser was seen as a well-rounded and sociable young man by his high school classmates and teachers. Chesser was exposed to Islam when he dated a Muslim peer. Once exposed, Chesser explored Islam through the Internet and immersed himself in the ideals and beliefs of the more radical Islamic groups. Expanding his involvement at a fast pace, Chesser was an active member of at least six different jihadist websites and chat forums. This behavior caught the attention of Jarret Brachman, a terrorism scholar, who engaged Chesser in conversation and coined the term 'jihobbyist' for people such as him, who are fascinated by Islam or jihad but were not members of

---

[55] Bob Drogin and April Choi, "Teen Held in Alleged Portland Bomb Plot," *Los Angeles Times*, November 28, 2010, http://articles.latimes.com/2010/nov/28/nation/la-na-portland-bomb-plot-20101128.

[56] Ibid.

[57] U.S. District Court for the District of Oregon, "Arrest Warrant: United States of America v. Mohamed Osman Mohamud," *Oregon Live*, November 26, 2010, http://media.oregonlive.com/portland_impact/other/USAFFIDAVIT.pdf, 3–9.

[58] Suzanne Kelly, "A Classic Case of Self-Radicalizing," *CNN*, February 28, 2012, http://security.blogs.cnn.com/2012/02/28/a-classic-case-of-self-radicalizing/.

recognized terrorist organizations.[59] Friends and family members noticed Chesser's views becoming more extreme. Additionally, in April 2010, Chesser wrote an email to Fox News, stating that he sought to "raise awareness of the correct understanding of key Islamic beliefs." In it he stated, "If you kill us, then we kill you."[60] Chesser set up several successful jihadist websites and a YouTube station dedicated to radical Islamic topics. Also in April 2010, Chesser warned via email the creators of South Park, Trey Parker and Matt Stone, of violent retribution for their depictions of Muhammad in their often irreverent cartoon. The post included the business addresses of likely targets of retribution, including Comedy Central as well as Parker and Stone's production company.[61] On July 10, 2010, Chesser was arrested while in the process of boarding a flight to Somalia. He told federal agents that he intended to train with Al-Shabaab, the terrorist organization in order to pursue further jihadist activities.

Looking at these three examples of lone-wolf terrorists, one can see several similarities and draw several general conclusions. First among these is that the lone-wolf mindset tends to be fostered over a long period of time. Humans are naturally social creatures and the process of developing a person into a non-social entity is not a fast one. Even with Zachary Chesser, who was the most quickly developed lone wolf in the case studies, it took several years from first contact with radical ideals to being considered a lone-wolf terrorist. In the case of Timothy McVeigh, the development of lone-wolf tendencies can be seen as far back as his early childhood. Obviously, not all neglected or socially backward individuals will resort to lone-wolf terrorism, but it is a strong prerequisite for the typology.

The second trend seen in these case studies and in the overall examination of lone-wolf terrorists is that they tend to show a much higher rate of psychological disturbances than other terrorists.[62] Statistically, terrorists in traditional hierarchical

---

[59] Jarret Brachman, *Global Jihadism: Theory and Practice* (London: Taylor and Francis Group, 2009).

[60] Joshua Rhett Miller, "Road to Radicalism: The Man Behind the 'South Park' Threats," *Fox News*, April 30, 2010, http://www.foxnews.com/us/2010/04/23/road-radicalism-man-south-park-threats/.

[61] Tom Lister, "Radical Islamic Website takes on 'South Park'," *CNN*, April 19, 2010, http://news.blogs.cnn.com/2010/04/19/security-brief-radical-islamic-web-site-takes-on-south-park/.

[62] Becker, "Explaining Lone Wolf Target Selection," 962.

groups show no higher incident of psychological problems than the public at large. Not surprisingly, lone wolves have a much higher rate of exhibiting such psychological problems as paranoia, obsessive-compulsive disorder, and severe depression.[63] As with the issue of socially withdrawn individuals, not all people with the psychological problems listed above are going to develop into lone-wolf terrorists; however, these psychological issues do appear to be another strong prerequisite for lone-wolf behavior.

Another trend that emerges from these case studies is the tendency of lone-wolf terrorists to provide signals of their intent prior to attacks. McVeigh wrote letters to local media with extremist viewpoints and contacted family members about paranoid suspicions. Chesser threatened the individuals he intended to target and, after the fact, his family members noted his withdrawal and change in personality over the preceding years. Of the three, Mohamud did the least telegraphing of his intentions of terrorist activities. His friends and family were surprised after his arrest since he appeared to be sociable and happy in his life. His example serves as a counterpoint and reminder that there is no rote path to lone-wolf terrorism. Becker and Teich's overall studies do show that the trend among lone-wolf terrorists is to provide clues to their violent intents in some form or manner. This trend is less compelling than either of the previous ones discussed but is still statistically significant. Highlighting this, Teich argues that lone-wolf terrorism, "is most difficult to prevent when the attacker has no contact whatsoever with other extremists – Pantucci's loners were seen to be the most successful at carrying out terrorist attacks."[64] Even those lone wolves that did provide clues prior to their attack did so in a much more subtle and less detectable manner than a traditional terrorist group. Often, lone wolves only transmit such clues to family or close friends, though there are cases such as McVeigh and Chesser in which the media or targets were contacted.

One typically held belief that can be dispelled by these case studies is the notion that all lone wolves are extreme recluses who completely eschew human contact in any form. While some such as McVeigh or Ted Kaczynski, the Unibomber, largely adhere to this preconception, the majority, though awkward in their social interactions, tend to have

[63] Spaaij, "Enigma of Lone Wolf Terrorism," 862.

[64] Teich, "Trends and Developments in Lone Wolf Terrorism," 22.

some sort of social network. Usually limited in scope, these networks are present none the less. This insight is important because it dispels the notion that lone-wolf terrorism cannot be prevented. In fact, Teich states that, "even though [lone wolves] are unaffiliated and thus harder to trace, their attacks are preventable." Becker expands on this notion in his conclusion by arguing that, "lone wolves are what might be called 'weak opportunists'. Lone wolves exhibit a propensity to strike at the intersection of their ideology and their daily routines … this tendency implies a special role for communities and local law enforcement agencies in monitoring at-risk individuals."[65] This is echoed by professional law enforcement such as Sir Bernard Hogan-Howe, commissioner of London's Metropolitan Police Service, when he stated that, "Although they're said to be lone wolves, they usually know someone who cares for them or they're in contact with, and those people will notice that type of change of behavior."[66] As such, clues about a pending lone-wolf attack will more likely be received by local citizens within a lone wolf's community than through national electronic surveillance efforts. This difference in signals means a different method of receiving those signals by authorities needs to be implemented.

D. CURRENT EFFORTS TO COMBAT LONE-WOLF TERRORISM

Law enforcement officials are not ignorant to the difference in indicators between lone-wolf terrorists and traditional hierarchical group attacks and have attempted to adapt their intelligence collection to this emerging threat. It is true that these new efforts have resulted in an evolution in intelligence actions by law enforcement and have seen a commensurate increase in prevention of lone-wolf terrorist incidents. Yet most of these innovations still adhere to an institutional tendency of top-down collection and as a result, suffer some of the same limitations as traditional intelligence methods.

One of the most common, successful, and widely publicized reforms in domestic intelligence is known as community outreach or community policing. Community outreach seeks to build trust within at-risk communities and develop cooperation with

---

[65] Becker, "Explaining Lone Wolf Target Selection," 971.

[66] Hays, "Lone-Wolf Terror Threat."

community members while simultaneously presenting counter-radical narratives.[67] Colloquially known as a return to the "beat cop," it emphasizes personal interaction between law enforcement and the communities they patrol. While a step in the right direction, this effort suffers limitations similar to other top-down methods of collecting information. Specifically, the resource investment, of both time and manpower, grows exponentially with any desired increases in coverage. This is because each beat cop is canvassing an area and pulling information from the citizens. They are individually establishing relationships with shop owners and community leaders, which takes time and effort. While these efforts have been shown to pay off, they will never be able to reach down to the level needed to canvass the majority of citizens in an area. While the most visible individuals, such as the store owners and community leaders, are being interacted with, the vast majority of citizens are not. The average stay-at-home mother, factory worker, or high school student will not develop a relationship with a beat cop executing community engagement because they are not one of the most visible and easily accessible community members. This limited community penetration results in large swaths of the population who will not receive the engagement of local law enforcement.[68] As such, these individuals will be left uncovered by this form of domestic intelligence gathering.

Traditional electronic surveillance has experienced an evolution of its own in response to increasingly insular nature of terrorist attacks. This has included broader mandates to collect on domestic targets such as the PRISM program and meta-data collection of cell phone calls as well as the non-standard approach of social media and chat room data scraping. Once again, the goal is to reach further into the fabric of U.S. society in an effort to identify potential threats earlier and prevent attacks on the populace. Unfortunately, electronic surveillance provides much larger amounts of data than can be processed at a central location. Analyzing every Tweet, Facebook post, and e-mail sent is too large a task. This fire hose of data can only be managed effectively when it is narrowly focused on an already identified target of interest and does poorly at

---

[67] Barnes, "Confronting the One-Man Wolf Pack," 1634.

[68] Jerome H. Skolnick and David H. Bayley, "Community Policing: Issues and Practices Around the World," *National Institute of Justice: Issues and Practices*, May 24, 1988, https://www.ncjrs.gov/pdffiles1/Digitization/111428NCJRS.pdf, 86.

wide canvassing for initial indicators.[69] This means that it provides an excellent tool of tracking and understanding an already identified person of interest but does little in helping with the initial identification of those individuals.

The various "See Something, Say Something" campaigns and associated tip lines is another emerging technique to reach further into society and extract the subtle indicators of lone-wolf activity. It is one of the most innovative and potentially useful methods seen so far. This effort relies on the grassroots ideal of pushing information from the masses up with small amounts of law enforcement interaction and oversight required when compared to community outreach. Assumed and expanded by DHS in 2010, after the New York Metropolitan Transportation Authority demonstrated it as a proof of concept, the See Something, Say Something campaign is designed to raise national public awareness of the indicators of terrorism and to encourage the public to report such indicators.[70] The biggest potential gains from a program such as this is the grassroots, ground up approach to acquiring information that can be turned into timely and actionable intelligence. By connecting the lowest level, the individual citizen, the program has the potential to exponentially expand the number of people monitoring the situation in the U.S. homeland.

Unfortunately, the See Something, Say Something program suffers from a few roadblocks that make its effectiveness less than optimal. First and foremost, the program is not well known by the public. A recent Gallup poll showed that fewer than half of U.S. citizens have even heard of the See Something, Say Something program. Additionally, less than twenty-five percent could accurately identify what the program was designed to do.[71] If most of the nation does not know the program's purpose or that it even exists, then the likelihood of the public knowing whom to contact and what information is pertinent is even lower. Even if we were to assume all of the U.S. public was aware of the

---

[69] Barnes, "Confronting the One-Man Wolf Pack," 1638.

[70] Department of Homeland Security, "If You See Something, Say Something," accessed May 23, 2014, http://www.dhs.gov/if-you-see-something-say-something.

[71] Steve Ander and Art Swift, "See Something, Say Something: Unfamiliar to Most Americans," *Gallup Politics*, December 23, 2014, http://www.gallup.com/poll/166622/something-say-something-unfamiliar-americans.aspx.

program, knew its purpose, and knew how to contact officials with information, it is still inhibited by a relatively high cost of participation for the citizen. Specifically, the time it would take to track down a police officer or research the correct local hotline to call for a suspicious event is likely to dissuade an individual from doing so. The fact that the program is very local in nature raises the cost of participation as well. Every city and region has a different hotline to call and has different requirements for information to provide. Even the most revolutionary part of the See Something, Say Something effort, reporting via mobile applications, has been diluted by this same localization and low exposure. Several mobile applications, such as New Jersey Office of Homeland Security and Preparedness' SAFE-NJ, excel technically, but receive only limited advertisement and explanation to the public. Additionally, a person commuting from Trenton, New Jersey to Philadelphia, Pennsylvania would need to use three different apps, with three different user interfaces, reporting to three different law enforcement agencies over the course of 30 miles. This localization of the initiative means that a method of reporting that a resident of Buffalo is familiar with is unlikely to apply should they visit New York City or other areas. The lack of awareness and high cost of participation have combined to make the See Something, Say Something program largely ineffective.

That being said, the idea behind and basic nature of the See Something, Say Something program has great potential if instituted correctly. The challenges it has faced are not intrinsic to the program itself but stem rather from poor funding, ineffective public relations campaigns, and implementation which fails to address the needs of either law enforcement or the citizens. The See Something, Say Something program's setbacks can illustrate quite clearly what steps need to be taken in the future to make such citizen-centric domestic intelligence efforts more successful. Specifically, it will need to be widely publicized and readily adopted by a large percentage of the population. It must be easy to use by the average citizen and require minimal time investment by participants. It will have to intrinsically engage the users in a manner that makes them want to participate in the program. Each of these solutions will be addressed in later chapters of the thesis in more depth but are mentioned here to illustrate the potential this already-

developed domestic intelligence program has in using crowdsourcing to combat lone-wolf terrorists.

This chapter examined the lone-wolf terrorist, its evolution from hierarchical terrorist groups, and the advantages and disadvantage inherent to lone-wolf tactics. It also examined the difficulties faced by law enforcement and intelligence services in detecting lone-wolf operators. Next, several case studies in which lone-wolf tactics were used by terrorists were laid out in an effort to identify early indicators of potential lone-wolf actions. The chapter concluded with an examination of current methods of identifying and preventing lone-wolf terrorists that are being implemented by law enforcement agencies in the United States. Deficiencies in the identification process inherent to both the current methods and proposed traditional solutions were explored. In summary, there are gaps in the traditional domestic intelligence system which lone-wolf terrorists, through their very nature, are able to more easily exploit to avoid detection than the traditional hierarchical terrorist groups the United States has been fighting for the past several decades.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CROWDSOURCING: LESSONS FROM COMMERCIAL APPLICATIONS

Yale University's Yochai Benkler states that industry "understands the world is becoming too fast, too complex and too networked for any company to have all the answers inside."[72] It is for this very reason that an increasing number of companies are turning to crowdsourcing as a way to innovate and solve problems at a pace and success rate never seen before. Crowdsourcing is a tool that holds promise not only for private enterprise but for any entity wishing to use it. This chapter addresses exactly what crowdsourcing is, why it is useful, and what problems it excels at solving. Case studies from several successful crowdsourcing endeavors will be examined to determine the qualities which have allowed them to succeed and contrasting their success with some instances in which crowdsourcing failed. Once the advantages and disadvantages of crowdsourcing have been examined, its applicability to domestic intelligence is examined to determine if crowdsourcing is a viable tool in detecting lone-wolf terrorist threats.

A. WHY CROWDSOURCING IS RELEVANT

Before addressing the question of how crowdsourcing can be used to collect domestic intelligence to stop lone-wolf terrorists, one must first address a more basic and underlying issue. Specifically, is using information willingly provided by the population at large a sound intelligence methodology? There are many in the intelligence field who would view such efforts as pointless since they believe that if a piece of information is not secret, then it is not intelligence. For them, intelligence is the process of collecting information known only to the adversary and to the intelligence experts, and which there is reasonable certainty that the adversary is unaware of the intelligence experts' possession of such knowledge. Under this view, whole domains of intelligence such as Open Source Intelligence (OSINT) are considered useless since the information is freely

[72] Adam Davidson, "Big Firms Eye 'Open Innovation' for Ideas," *National Public Radio*, May 27, 2007, http://www.npr.org/templates/story/story.php?storyId=10480377.

available to most of the population and because the adversary can be reasonably assured that the intelligence experts possess the information.[73]

It is certainly true that the value of intelligence increases inversely with the number of people who know it. Known only to a few, intelligence can be of much greater value than if the same information were widely disseminated. One only need consider industrial capabilities of countries engaged in economic negotiations to realize that there is still much intelligence value even for widely known pieces of information. In those same economic negotiations, knowledge of the other county's industrial capabilities is still a useful bargaining chip even when the other country is aware the knowledge is available to both parties.

In the end though, whether information provided by the population can be considered intelligence is largely a moot point since it is still valuable information for a variety of reasons, whether considered intelligence or not. The Times Square bombing of 2010 was prevented by a local street vendor tip to law enforcement.[74] In 2014, an intended school massacre in Waseca, Minnesota, was thwarted by a stay-at-home mother who saw suspicious activity through her kitchen window.[75] In 2002, bystander information from multiple sources, including a priest and a truck driver, directly led to the localization of the Beltway Snipers.[76] These real-world events provide proof of the usefulness of citizen intelligence in detecting and preventing lone-wolf terrorism.

Foremost, using the U.S. citizenry as intelligence collectors expands the domestic intelligence network exponentially. In 2008, the population of the United States was over 304 million people with approximately 765,000 law enforcement officers employed in

---

[73] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2012), 112–113.

[74] Alison Gendar , Rocco Parascandola , Kevin Deutsch , and Samuel Goldsmith, "Time Square Car Bomb: Cops Evacuate Heart of NYC After Potential Terrorist Attack," *New York Daily News*, May 1, 2010, http://www.nydailynews.com/news/crime/time-square-car-bomb-cops-evacuate-heart-nyc-potential-terrorist-attack-article-1.444423.

[75] Pat Pheifer, "Waseca Teen Accused in School Shooting Plot had been Planning for Months," *Star Tribune*, May 10, 2014, http://www.startribune.com/local/257505631.html.

[76] Rona Kobell, "For Sniper Tipster, Small Rewards," *The Baltimore Sun*, December 13, 2003, http://articles.baltimoresun.com/2003–12–13/news/0312130235_1_montgomery-county-donahue-sniper.

the United States during the same time.[77] This provides coverage of approximately one officer for every 400 people nationwide. Additionally, as of October 31, 2013, the FBI employed a total of 35,344 people, only 13,598 of which were special agents. If only 10 percent[78] of the U.S. population participated in crowdsourced domestic intelligence collection, it would represent coverage and community penetration forty times the level achievable using only law enforcement to collect the same intelligence. This pervasiveness is needed to detect the much more subtle signals which lone-wolf terrorists provide and which they tend to distribute to a much smaller group of people.

Not only does citizen collection of intelligence increase the pervasiveness of intelligence for law enforcement, it also greatly enhances the persistence of collection. A law enforcement officer conducting community outreach will only be able to reach a limited subset of high-visibility individuals in a given community. Each interaction the officer performs will be limited in scope and time based on limited time and resources allocated to such efforts. Contrast this with individuals in the community who are constantly embedded and, for approximately sixteen hours a day, are conscious observers of their surroundings and fellow citizens. This persistence is crucial because it gives the collector a higher likelihood of detecting signals of impending attacks and provides them more familiarity with their surroundings. This naturally leads to the final advantage of using citizens for collection: local expertise.

Local expertise is important because it is only by knowing what is normal or belongs in an area that a person can then determine what is out of place. To an individual thrown into a foreign land for the first time, everything appears new and out of place because they are unfamiliar with local methods and traditions and they carry preconceived notions with them of what they consider normal from their own culture. Likewise, officers patrolling a neighborhood that they are not a member of may not

---

[77] United States Census Bureau, Population Estimates, October 09, 2012, http://www.census.gov/popest/data/intercensal/national/nat2010.html.

Brian Reaves, "Census of State and Local Law Enforcement Agencies, 2008," Bureau of Justice Statistics, July 2011, http://www.bjs.gov/content/pub/pdf/csllea08.pdf.

[78] Charles Arthur, "What is the 1% rule?," *The Guardian*, July 19, 2006, http://www.theguardian.com/technology/2006/jul/20/guardianweeklytechnologysection2.

notice things that are out of place. Additionally, because they are viewed as outsiders, local citizens may be less forthcoming with information or act more guarded around law enforcement than they might with other local citizens. As such, local citizens will be able to get a more accurate view of what is normal for a community and are more likely to be given unguarded access to people's actions and thoughts. This combination of pervasiveness, persistence, and local expertise make the concept of using local citizens for domestic intelligence collection very attractive.

In this respect, crowdsourcing should be seen as a tool to achieve this citizen collected domestic intelligence strategy rather than a strategy in and of itself. Crowdsourcing is, "an online, distributed problem-solving and production model that leverages the collective intelligence of online communities to serve specific organizational goals. Online communities, also called crowds, are given the opportunity to respond to crowdsourcing activities promoted by the organization, and they are motivated to respond for a variety of reasons."[79] Broken into its basic components, scholars have reached an agreement that for a task to be considered crowdsourcing, it must have the following four key ingredients: an organization with a task which needs performing, a community that is willing to perform the task voluntarily, an online environment that allows interaction and work to take place, and mutual benefit to both the organization and community.[80]

Soliciting a large group of people for ideas and information is nothing new. "In 1714, the British established a commission offering 20,000 pounds (roughly $12 million today) to anyone who could invent a way to determine longitude on a sailing vessel."[81] Top scientific minds of the time, including Isaac Newton, had failed. The solution, an extremely precise clock, was developed by an uneducated cabinetmaker from Yorkshire. Crowdsourcing, according to Brabham's definition, is a phenomenon that is related but much more specific. Specifically, crowdsourcing deals exclusively with collaboration through the Internet. No other medium is able to link such a wide array of people at all

[79] Brabham, *Crowdsourcing*, xix.

[80] Ibid., 3.

[81] Howe, *Crowdsourcing*, 146–147.

levels so quickly, efficiently, and tightly as the Internet. Additionally, the Internet comes closest to providing an environment for true meritocracy. On the Internet, what a person looks like or sounds like no longer matters. The only thing that holds value is the content of a person's ideas. The ability to quickly and easily build a large community with an intrinsic anonymity provides the ideal environment for distributed collaboration in a way never seen before.

Under the broad definition of crowdsourcing, several sub-categories emerge that help experts better define specific endeavors into the realm. Several scholars have created different categorizations based on competing factors such as the type of organization employing crowdsourcing, size of community, or length of project. Brabham takes a different approach and develops a typology of crowdsourcing based on what, in general terms, the project is setting out to accomplish. This is the most useful definition and is the typology used in this thesis. Brabham breaks crowdsourcing into four distinct types: knowledge discovery and management, broadcast search, peer-vetted creative production, and distributed human-intelligence tasking.[82]

Of these four categories, knowledge discovery and management as well as distributed human-intelligence tasking will be relevant to the crowdsourcing of domestic intelligence. The other two deal with the creation of new products or solving of empirical problems, neither of which intelligence collection and processing fits into. Knowledge discovery and management tasks a crowd with finding and collecting information into a common location and format.[83] This would be analogous to calling several people and asking them what the weather is at their location in order to gain a picture of the current climate conditions across a wide region. The mobile navigation application Waze will be used as the case study for this type of crowdsourcing. It should serve as guidance for the portion of crowdsourcing domestic intelligence which interfaces with the U.S. citizenry and will provide insight on how to gainfully engage the community for such tasks.

[82] Brabham, *Crowdsourcing*, 45.

[83] Ibid.

Distributed human-intelligence tasking asks a crowd to analyze large amounts of information in cases where human intelligence is more efficient or effective than computer analysis.[84] Pattern recognition, audio transcription, and picture identification are all tasks which fall into this category and which are among the tasks performed by people participating in Amazon's Mechanical Turk (MTurk). MTurk will therefore be used as the second case study of crowdsourcing in the private sector. It will provide a template for the backend of a crowdsourced domestic intelligence effort by highlighting key ways to process information which is typically difficult for automated systems.

The third case study, DARPA's Ten Red Balloons experiment, though not strictly commercial in nature, has a large amount of relevance to domestic intelligence. The experiment highlighted the huge gains in speed and efficiency in locating difficult to find and geographically distributed objects through the use of crowdsourcing. The lessons learned from Ten Red Balloons should reinforce the strengths of crowdsourcing and provide as near a direct real-life example of crowdsourcing domestic intelligence as is currently available.

B. CASE STUDIES OF CROWDSOURCING

Waze, a mobile navigation application for use on smart phones, was launched in 2008 and quickly became one of the most successful navigation applications on the market. So much so that in 2013, Waze's largest competitor, Google, purchased Waze Ltd for $966 million.[85] Waze is set apart from the myriad of other navigation applications available commercially by its crowdsourcing components. The utilization of crowdsourcing has enabled it to be more accurate and adaptable than its competitors and has been directly attributed to its huge success.[86] At its most basic level, Waze participants passively provide data to central servers about their current location and speed. Using this data, Waze is able to provide real-time information on traffic flow and

[84] Ibid.

[85] Dara Kerr, "Google Reveals It Spent $966 Million in Waze Acquisition," *CNET*, July 25, 2013, http://www.cnet.com/news/google-reveals-it-spent-966-million-in-waze-acquisition/.

[86] Rip Empson, "WTF Is Waze And Why Did Google Just Pay A Billion+ For It?" *TechCrunch*, June 11, 2013, http://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/.

congestion for a covered region, highlighting slowdowns with yellow and standstills with red. Additionally, algorithms within Waze can use this data to route motorists around heavily congested areas and provide the most efficient commute possible. When Waze initially expands into an area it also uses this passively-provided user data to verify pre-existing, and usually dated, map data. Waze will display Pac-man like dots on any unverified roadways for users to drive over. Driving on them provides users with points and provides the database verification that the road is still passable.

This passive collection of data only scratches the surface of Waze's crowdsourcing abilities. Waze also allows the community to participate in a much more active manner. A driver, through a few quick taps, may log such traffic incidents as accidents, debris on the road, police, or inclement weather. Participants are awarded points and the data is fed into central servers and distributed to all other Waze users in the area. When nearing any of these user-generated alerts, Waze gives the other users the option of either confirming its existence or reporting the condition resolved. This peer review allows continuous updates while simultaneously self-policing errant reports. Using this system, users can easily see which alerts have been most recently updated and which ones have the most confirmations from other users. This provides instant graphical feedback to all users on the validity of any alert in their area.

At the most involved level, users can log into the Waze system on a computer and make a formal report on road changes. This can include anything from a newly constructed roadway or a closure of a semi-permanent nature. This interaction requires review by Waze personnel but can be verified and incorporated into the Waze database in less than five days. Bradley Horowitz postulated the 1:10:89 rule, which states that for any crowdsourcing effort, 1 out of 100 people will fall into this deep-use category, 10 out of 100 will vote on content and participate at a shallow level, while 89 out of 100 will simply consume the content developed by others.[87] This deep level of participation by the one percent rewards them with unique avatars and badges which are unavailable any other way. There are additional and very powerful intrinsic motivations in play as well.

[87] Howe, *Crowdsourcing*, 227.

When one power-user was asked why he spent 50 hours a week for almost two years helping to map the country with 378,000 edits to maps for free, he responded by saying, "You feel good about knowing that the people who drive around every day save time because you are investing your time in fixing the roads and doing this mapping."[88]

The points, levels, and avatars listed above are all forms of gamification, "the use of game thinking and game mechanics in non-game contexts to engage users in solving problems,"[89] and they are integral to Waze's model of operation. By providing users with virtual awards and recognition for performing tasks which are mundane but beneficial to the company and the community, they are incentivizing users to work for the company at a very low cost. Giving a user's avatar a crown for reporting a certain number of traffic incidents costs Waze nothing but it provides the user a representation of his accomplishment, which he can see and which his fellow participants can see and covet as well. This award system spurs further participation and if done correctly, can help overcome one of the most common problems most crowdsourcing projects encounter, reaching a critical mass of participants to make the project viable.

Waze, and many other crowdsourcing projects, have implemented social media integration to also assist in building a user base.[90] The grassroots nature of crowdsourcing means that word of mouth is usually the predominant form of marketing and social media can turn provide this word of mouth a megaphone to get the message out. Waze links to a user's Facebook account and allows direct competition for new badges and awards between people who know each other in real life rather than just providing an arbitrary ranking on a global leader board. Users linked through Facebook are also able to send each other messages via Waze and synchronize travel to a common destination by viewing each other's estimated time of arrival. By integrating social media, Waze has made the gamification more personal for the user and thereby ensuring

---

[88] Matt McFarland, "Why Waze is so incredibly popular in Costa Rica," *The Washington Post*, October 24, 2014, http://www.washingtonpost.com/blogs/innovations/wp/2014/10/27/why-waze-is-so-incredibly-popular-in-costa-rica/.

[89] Deterding, "From Game Design Elements to Gamefulness," 10.

[90] Roy Furchgott, "Filling in Map Gaps With Waze Games," *The New York Times*, May 6, 2010, http://wheels.blogs.nytimes.com/2010/05/06/filling-in-the-map-gaps-with-waze-games/.

wider and more frequent participation.[91] Further case studies will show this building of a community with interaction and transparency to be one of the biggest factors in making a crowdsourcing project successful. Should it adopt a crowdsourced domestic intelligence effort, this will present the intelligence community, known for its closed nature and lack of public interaction, with one of its biggest challenges.

Launched by Amazon in 2005, Mechanical Turk (MTurk) is a crowdsourcing project designed to harness human computation ability to perform tasks which computers are ill-suited for.[92] MTurk was originally used in-house by Amazon to cull duplicate descriptions of items sold on their website. They then expanded its application by allowing outside entities to solicit jobs to be completed by MTurk participants. These jobs vary from photo identification, to transcription, or survey completion. Most are tasks which computers are ill-suited at, such as determining a pepperoni pizza from a cheese pizza in a picture.[93] Additionally, each individual task tends to be very short in duration. This microtasking philosophy allows businesses to harness people's spare time while benefiting the individuals with a minor secondary income and a sense of accomplishment.[94] Organizations submit job requests through the MTurk website and participants can then select jobs from the listings which they feel particularly suited for or interested in. Once complete the originating entity reviews participant's work and either accepts or rejects it. A participant's acceptance rating can then guide follow-on entities in accepting participants with a proven track record for their tasks. This community feedback is critical in ensuring that a high quality is maintained.

MTurk differs from Waze in that the reward is extrinsic, in the form of monetary payments, rather than intrinsic. This extrinsic reward system gives MTurk an advantage in workers accepting a task and increasing the speed with which it is completed; however, research has concluded that these extrinsic rewards have no bearing on the

---

[91] Ibid.

[92] Ellen Cushing, "Amazon Mechanical Turk: The Digital Sweatshop," *Utne Reader*, January 2013, http://www.utne.com/science-and-technology/amazon-mechanical-turk-zm0z13jfzlin.aspx#axzz3HvYkp0Uo.

[93] Basulto, "Humans Are the World's Best Pattern-Recognition Machines."

[94] Cushing, "Amazon Mechanical Turk."

quality of work done.[95] Rather, problems typically framed with intrinsic rewards, such as helping others, are shown to have higher quality work associated with them. Most importantly, the researchers found a synergistic interaction between intrinsic and extrinsic motivators. Combining extrinsic and intrinsic rewards has been shown to increase the acceptance rates for tasks as well as producing higher quality outputs.[96] These findings translate to other crowdsourcing projects and can help guide a crowdsourced domestic intelligence effort in attracting participants and encouraging a high quality of inputs from those participants. MTurk's ability to harness human processing also shows promise for crowdsourcing some of the initial analysis of intelligence data, not just collection. Peer review of submitted alerts could provide reinforcement for a valid alerts importance and help cull inputs with less relevance.

The final case study of a successful crowdsourcing project is not of a commercial nature. DARPA's Ten Red Balloons experiment in human networking was launched in December of 2009 by the government organization as a way to explore the roles the Internet and social networking play in real-world communication and collaboration.[97] In the competition for a $40,000 prize, teams had to locate ten red balloons placed around the United States and then report their findings to DARPA. The contest creators intentionally left the format and methodology of the search vague in order to push such decisions down to the participants. Strictly speaking, neither teams nor social networking needed to be used by participants, though all the top competitors used both heavily. The winning team, a group of 5 students from MIT who found out about the competition four days prior to it starting, provides an excellent example of the power crowdsourcing brings to bear on such real-world problems. The MIT team found all ten balloons in less than

---

[95] Jakob Rogstadius, Vassilis Kostakos, Aniket Kittur, Boris Smus, Jim Laredo, and Maja Vukovic, "An Assessment of Intrinsic and Extrinsic Motivation on Task Performance in Crowdsourcing Markets," *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*, July 05, 2011, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2778/3295, 321.

[96] Ibid.

[97] Doug Gross, "MIT Wins $40,000 Prize in Nationwide Balloon-Hunt Contest," *CNN*, December 07, 2009, http://www.cnn.com/2009/TECH/12/05/darpa.balloon.challenge/index.html?_s=PM:TECH.

nine hours, a task which DARPA had estimated would take approximately two weeks.[98] Developing a pyramid scheme method of reward, the team allocated half the prize money to those individuals who gave them proof of the locations of the ten balloons and then used the other half of the prize money to reward those individuals who referred the balloon finders to the competition, those who referred the referrer, and so on in decreasing increments. This method of reward created motivation for a self-propagating network of individuals with a motivation to not only search for the balloons but to also recruit other individuals to the project. This method of recruitment is very effective in building a motivated and involved user base very quickly.

Closely related to the DARPA Ten Red Balloon experiment is another experiment conducted by *Wired Magazine* in which a reporter attempted to remain hidden from public view for a month.[99] This contest also offered a monetary prize and also left the methods of competition purposely vague. Once again, individuals self-organized into teams which coordinated using social media and the Internet.[100] The winning team was able to locate and confront the reporter with their findings in 25 days, an astonishing feat considering the boundaries of the search were the continental United States. This competition, like DARPA's Ten Red Balloons, highlights the importance of the social aspect of such endeavors. "Teams appear to have developed a strong social cohesion – individuals likely became interested in participating and assisting because they wanted to help the group."[101] While these findings simply reinforce the results of other crowdsourcing projects, they differ in that they were seeking objects or individuals in the real world and were able to do so extremely quickly and efficiently when compared with traditional methods. This sort of search is directly applicable to any efforts at crowdsourcing of domestic intelligence.

---

[98] Christopher M. Ford, "Twitter, Facebook, and Ten Red Balloons: Social Network Problem Solving and Homeland Security," Homeland Security Affairs, vol 7, art 3, February 2011, http://www.hsaj.org/?fullarticle=7.1.3.

[99] Evan Ratliff, "Vanish: Finding Evan Ratliff," *Wired Magazine*, August 14, 2009, http://archive.wired.com/vanish/2009/08/author-evan-ratliff-is-on-the-lam-locate-him-and-win-5000/.

[100] Ford, "Twitter, Facebook, and Ten Red Balloons."

[101] Ibid.

C. APPLICABILITY OF CROWDSOURCING TO DOMESTIC INTELLIGENCE

Combined, these case studies highlight several key aspects to crowdsourcing as a technique for gathering intelligence. The most important and perhaps the least intuitive fact is that crowds almost always outperform experts in the field. Howe makes the argument that, "the many can work together to outperform the few," and further expounds later that, "the crowd will almost always outperform any number of employees."[102] Brabham echoes this sentiment when contemplating crowdsourcing in the scientific community by saying that, "the perspectives and internal problem-solving heuristics of outsiders allow them to see novel solutions to problems that experts at the center of a scientific domain may not be able to see."[103] Combined with an expertise and familiarity with local customs and routines, this outsider's perspective to problem solving has the potential to allow local citizens to perform as adept suspicious activity detectors. Unencumbered by what is traditionally seen as indicators of threats, local citizens may see and interpret threats that an expert in law enforcement may not. By combining a crowdsourced methodology with the expertise and assets of traditional intelligence operators, a crowdsourced domestic intelligence program would allow the experts to focus on connecting the dots, managing the process, and coordinating with other sources of intelligence rather than acting as the boots on the ground in the collection of lone-wolf terrorism indicators. The intelligence professionals are not superseded with this process. Rather, they are augmented and reinforced by a network of actively involved citizens.

The second advantage these cases highlight is the large successes obtained by bringing large amounts of manpower to bear on large problems. While this in itself is fairly intuitive, what is striking is the ease with which such coordination of massive amounts of people can be accomplished thanks to the connectivity and automation inherent to the Internet. The winning team from DARPA's Ten Red Balloons challenge only found out about the contest a few days prior and was able to organize a network of thousands of active and motivated participants into a cohesive team within that short time

[102] Howe, *Crowdsourcing*, 11–12.

[103] Brabham, *Crowdsourcing*, 21.

period.[104] Once the contest began, that same team was able to coordinate with those same thousands of participants in real time, collecting and analyzing data at rates which would be unachievable without the Internet. "The short-term growing pains that will surely accompany a transition [to crowdsourcing] will be outweighed, I believe, by the long-term benefits of a flattened environment in which we will all become valuable contributors."[105] This is largely due to the fact that, "the amount of knowledge and talent dispersed among the numerous members of our species has always vastly outstripped our capacity to harness those invaluable qualities."[106] This sort of efficiency in coordination and flattening of the organizational structure will be critical in any large project connecting a widely distributed group of participants such as a nationally coordinated, citizen-dependent intelligence effort.

Motivation of participants is another key factor which all of these successful crowdsourcing efforts have in common. Whether it is through a more traditional method such as the nominal salary that MTurk provides or the gamification approach that Waze uses, all the projects acknowledge that motivation of participants is critical in crowdsourcing. Due to political and economic constraints, it is unlikely that a domestic intelligence effort will be able to use the most traditional motivation, salaries. As such, the focus of the discussion in Chapter IV on motivation, as it applies to crowdsourced domestic intelligence, will necessarily be on such approaches as rewards based systems and gamification. Chapter IV also examines methods to exploit people's internal motivations of increased personal security and a desire to assist the local community. This focus on internal motivations has definite advantages since studies have shown that problems framed with intrinsic rewards, such as helping others, are shown to have higher quality work associated with them.[107]

One of the disadvantages experienced in crowdsourcing is that a poor start is very difficult to bounce back from. This is due to the heavy reliance on community building

---

[104] Ford, "Twitter, Facebook, and Ten Red Balloons."

[105] Howe, *Crowdsourcing*, 19.

[106] Ibid.

[107] Rogstadius, "Assessment of Intrinsic and Extrinsic Motivation," 321.

and participation inherent to crowdsourced projects. This emphasis on and need of a community presents a paradox of sorts for developing crowdsourced projects. They need a vibrant and active community to attract participants but they need a critical mass of participants to create an active and vibrant community. Assignment Zero, an early attempt at crowdsourcing investigative journalism, suffered from this very paradox, resulting in early termination of the project.[108] Assignment Zero built the required framework to host and engage a community of citizen journalists, but without an established forum with moderators and content in place, visitors rarely returned for a second visit and even more rarely contributed. Learning from this mistake and many others like it, a crowdsourced intelligence effort would need to seed a community via other means such as employees dedicated to cultivating community involvement and pre-established content ready for consumption by participants on day one. What such content might consist of in a domestic intelligence setting is addressed in Chapter IV.

Another significant disadvantage inherent to crowdsourcing is the reduced control the parent organization can exert when compared to traditional methods of managing labor. "The crowd wants to feel a sense of ownership over its creation, and is keenly aware when it is being exploited. The company, in this context, is just one more member of the community."[109] This need for transparency will be the largest hurdle the intelligence community will face in implementing a crowdsourced intelligence effort due to its very insular and secretive nature. The intelligence community's desire to keep as many things secret as possible is in direct conflict with the openness required in successful crowdsourced efforts. Brabham maintains that, "relationships between organizations and stakeholders are usually strongest when they are mutually beneficial, when they are symmetrical and communication flows two ways."[110] Howe acknowledges that this shift in thinking is not easy, even for private enterprise but maintains that it is the core of any successful crowdsourcing effort. "What unites all successful crowdsourcing efforts is a deep commitment to the community. This entails much more than lip service

[108] Howe, *Crowdsourcing*, 214.

[109] Ibid., 15–16.

[110] Brabham, *Crowdsourcing*, 109.

and requires a drastic shift in the mind-set of a traditional corporation."[111] This need for transparency and two-way communication in crowdsourcing efforts is one of the two major reasons that the local See Something, Say Something mobile applications have failed, along with lack of public attention. Those who participate using such programs as SAFE-NJ provide information to law enforcement but are not engaged or encouraged to further participate. It is a one-way street to a black hole into which they provide their information. This kind of mechanism breeds disinterest and disuse. If the intelligence community can come to terms with the requirements for transparency and two-way communication, while at the same time maintaining the secrets needed for national security, then it could have access to a new and powerful tool in its arsenal to combat lone-wolf terrorism.

[111] Howe, *Crowdsourcing*, 15.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. APPLYING CROWDSOURCING TO DOMESTIC INTELLIGENCE

Chapter II examined the problem of detecting lone-wolf terrorist activities prior to their acts being carried out. It attempted to distill those indicators which current domestic intelligence methods are ill-equipped to identify and examine why these methods are not suitable for the unique threat of lone-wolf terrorists. Chapter III provided an overview of crowdsourcing as a solution to a host of commercial problems and ways the private sector has harnessed this new tool. It also highlighted the advantages a crowdsourced approach brings to problem solving as well as pitfalls that crowdsourcing must avoid in order to be successful. Chapter IV matches the problem of identifying lone-wolf terrorist indicators with crowdsourcing as a method of solution by first examining in detail the nascent domestic intelligence crowdsourcing efforts currently in existence and determining why they have had limited success. Chapter IV then provides a template for a robust and responsive domestic intelligence crowdsourcing program that uses commercial crowdsourcing successes to guide it. It concludes by outlining the benefits, both immediate and ancillary, that such a program would provide to the law enforcement and intelligence communities.

A. CURRENT DOMESTIC INTELLIGENCE CROWDSOURCING ATTEMPTS

A search through the iTunes and Android app stores yields over one hundred different mobile applications for the reporting of criminal and suspicious behavior to law enforcement. This plethora of applications that are freely available to smart phone users, most offered and endorsed directly by different law enforcement agencies, confirms that the potential benefits of crowdsourced domestic intelligence is seen by the establishment. Were benefits not anticipated by law enforcement by such a program, then the limited time, resources, and effort of these local and often underfunded organizations would not have been invested in such a new and unproven method of intelligence collection. Even with this large interest by law enforcement, there have been few tangible results, either arrests or prevention of crime, due to mobile application reporting. A search of news

articles on crime prevention and arrests relating to mobile crime reporting applications from the past two years yields only two U.S. incidents in which mobile application reporting led directly to an arrest.[112] The question one must ask is, if crowdsourcing has successes at solving other problems and law enforcement has shown interest in using it for domestic intelligence, then why is it failing to yield any results?

There are several related and overlapping issues which have contributed to the poor performance of current domestic intelligence crowdsourcing attempts but they all revolve around the fact that officials are attempting to use crowdsourcing without understanding its strengths and weaknesses and failing to learn from commercial successes and failures with crowdsourcing. Foremost, law enforcement officials are viewing crowdsourced intelligence as simply an additional conduit of their established community reporting method, crime prevention hotlines. Though there are similarities, at its heart a crowdsourced effort at problem solving is based around community involvement and requires two-way communication.[113] All of the domestic intelligence applications examined for this thesis provided only one-way communication. In all the applications, a citizen reports suspicious or criminal activity via the app to law enforcement. The report is processed, analyzed, and investigated by officials but there is no means of providing feedback to the citizen. Few of the apps even provided a read-receipt acknowledging successful transmittal of the information. This lack of interaction and opacity in the process fails to elicit repeat interactions and does not engage the user.

The second major roadblock encountered by current domestic intelligence crowdsourcing efforts is the fragmentation of their efforts and hence the small scale of each individual effort. Most of the applications reviewed only cover a single county or major city while SAFE-NJ, the broadest reaching of them, covers the state of New Jersey. This fragmentation causes confusion for the citizens, which contributes to low adoption

---

[112] Terri Sanginiti, "Crime Tip App Leads to Drug Arrest," *Delaware Online News Journal*, October 8, 2014, http://www.delawareonline.com/story/news/crime/2014/10/08/crime-tip-app-leads-drug-arrest/16921703/.

Harris County Sheriff's Office, "iWatchHarrisCounty App Users Do It Again; Tips Lead to Drugs and Arrests," *Nixle*, October 23, 2013, https://local.nixle.com/alert/5290183/.

[113] Howe, *Crowdsourcing*, 15.

rates. Fragmentation also results in disjointed efforts by law enforcement due to disaggregated data collection. Criminals and terrorists do not abide by city limits and municipal boundaries. Information provided by one local domestic intelligence app is transmitted only to the local law enforcement office in charge of that app. It is then up to that law enforcement office to distribute the information to those other agencies which it feels is in need of it. This method of distribution usually involves a human in the loop and as such, is much more tedious and prone to errors than an automated system. This is the sort of problem highlighted by the 9/11 Commission's report on the failures of the intelligence community to stop those terrorist attacks. This fragmentation leads to a structural failure to connect the dots.[114] The information may be known to some select group of people but if the right people don't know it, then it isn't actionable.

The third hindrance to current efforts at crowdsourcing domestic intelligence stems from poor public relations and public awareness. Crowdsourcing is a human behavior and not a technology, though it requires technology to occur.[115] As such, for it to be effective, one needs the human element to participate in the endeavor. Recent attempts have faltered because of a lack of awareness by the public at large. Sporadic radio advertisements and a few billboards have been the method most commonly used to promote these local crowdsourced intelligence efforts and have failed to reach a large section of the population or capture the interest of the ones who were exposed to the advertising.[116] In some ways, this is a secondary roadblock resulting from the fragmentary approach law enforcement is taking. When each agency develops their own reporting app, they must each individually manage it and promote it as well. This results in duplicated public relations costs for agencies which do not have large budgets for such projects in the first place. These factors lead to poorly designed advertising with limited release and contribute to the small adoption rates by citizens.

---

[114] 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, (Washington, DC: United States Government Printing Office, 2004), http://govinfo.library.unt.edu/911/report/911Report.pdf, 408.

[115] Howe, *Crowdsourcing*, 11.

[116] Evan MacDonald, "Five Months After Launch, Use of Crime Tips App Low in Northeast Ohio," *Cleveland.com*, October 23, 2013, http://www.cleveland.com/metro/index.ssf/2013/10/five_months_after_launch_use_o.html.

The one thing most of the reporting apps have successfully adopted from civilian crowdsourcing efforts is the ability to lower the cost of participation for the users. The majority of people in the United States own a smart phone and the smart phone plays a large part in how they interact with the world.[117] They are comfortable with the form and function of such a device so that the addition of an application for reporting suspicious activity would not require a long education process; most of the current reporting applications are very user friendly and intuitive. Each of the three reporting apps tested for this thesis took less than fifteen seconds from opening to sending of basic informational reports. If personal identification, location data, and a picture were added, the time to report averaged between 20 and 30 seconds. Users are much more likely to participate and contribute to any effort if doing so only requires minimal time and effort on their part. This ease of use is paramount to maintaining an active user base. While the previously discussed pitfalls should be avoided by any future efforts at crowdsourced domestic intelligence, this reduction in the cost of participation should be emulated.

In summary, the current attempts at crowdsourced domestic intelligence have failed because they ignore or poorly address most of the tenets of establishing a successful crowdsourcing effort. These tenets have been learned through trial and error over the past several years by the private sector but are widely documented and easily implemented at this point in time. Any future attempts at crowdsourcing domestic intelligence should pay special heed to the lessons learned from previous crowdsourcing endeavors instead of attempting to reinvent the wheel.

B. A NATIONAL CROWDSOURCED DOMESTIC INTELLIGENCE ENTERPRISE

As it stands now, law enforcement has taken its first embryonic steps into the realm of crowdsourcing. The value and efficiency crowdsourcing brings to problems has been recognized and adopted in many places as an alternative source of domestic intelligence for crime prevention. Failure to recognize that a crowdsourcing solution requires a unique approach and a tailored environment have hampered current efforts.

[117] Aaron Smith, "Smartphone Ownership 2013," *Pew Research Internet Project*, June 5, 2013, http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013.

Using the lessons from these failures and the lessons outlined in Chapter III of the successes in commercial crowdsourcing efforts, this thesis will now provide a feasible, robust, and flexible approach to crowdsourcing domestic intelligence.

Of prime importance is the need for any new system to be national in nature. The Department of Homeland Security (DHS) is poised in an ideal position to take the lead of such an effort. DHS is a national organization with federal funding much greater than any local or state law enforcement agency and has direct contact and cooperation with all other organizations interested in domestic intelligence, from the national level down to local law enforcement. DHS is an entity large enough to manage such a national effort but is not so enmeshed with current intelligence operations, like the CIA or NSA, that a crowdsourcing effort would be automatically dismissed by the public. Nationwide coverage by a single program is of paramount importance for several reasons. Nationalizing the crowdsourcing effort pools resources and prevents overlaps and inefficiencies by all parties involved. It is much less expensive to have one major and fully-capable public relations staff managing a national campaign than the sum total cost of hundreds of local and often ad hoc attempts at advertising for such efforts. One voice with one message prevents confusion by the public as well. Citizens no longer have to wade through pages of suspicious activity reporting apps on their mobile phone trying to find their local one. Additionally, the public will feel more secure knowing that the program they are using has been nationally vetted and trusted. This feeling of security will translate to people being more likely to download and use such a program.

On the backend of the program, nationalization will have several useful advantages as well. A single database receiving all inputs from every user in the United States results in a much larger pool of data for analysis and comparison. As stated previously, terrorists and criminals do not adhere to municipal or state boundaries. Similar suspicious activity noted in several different geographic locations will have a much better chance of being correlated if all the information is in one database. With current programs, this merging of data happens manually and slowly at best or, at worst, not at all. With the power and sophistication of big data management available with today's technology, this glut of data need not result in information overload. Using

simple time and location filters, any organization with access to the data, from local law enforcement to national intelligence agencies, can view and manipulate only the data they find relevant and useful to them. While all parties would retain the ability to view the entire database, the ability to filter certain information would make it more manageable and relevant to the smaller law enforcement units. Embedded in the database management of such a program would be algorithms automatically searching for similar or related reports in the entire database. "Sophisticated analytics can substantially improve decision making, minimize risks, and unearth valuable insights that would otherwise remain hidden."[118] These algorithms would help connect the dots even if every organization viewing the data chose to self-impose blinders and only analyze the pieces of data emanating from their geographic region.

Nationalizing the crowdsourced domestic intelligence enterprise would also more easily tie it into other forms of intelligence. This ability to tie disparate reports from different sources is especially important in the search for such elusive targets as lone-wolf terrorists. As was shown in Chapter II, lone wolves are even more prone to slipping through the cracks of traditional detection than traditional terrorist groups and require officials to detect the more subtle clues they provide. Instead of linking databases of other intelligence to hundreds of local efforts individually, a national database would be a one-stop location for all other forms of intelligence to draw upon and contribute to.

The second key change that needs to be implemented in any new domestic intelligence crowdsourcing efforts is the interaction between the program and the citizens. While current mobile reporting applications have excelled at lowering the cost of participation by making the experience simple, fast, and anonymous, they have fallen short in the most critical of crowdsourcing needs, building a community of participants. Crowdsourcing thrives in an environment of two-way communication and transparency.[119] These requirements are the antithesis of traditional intelligence beliefs and it is therefore not surprising that previous crowdsourcing efforts for domestic

---

[118] Manyika and Chui, *Big Data*, 99.

[119] Brabham, *Crowdsourcing*, 109.

Howe, *Crowdsourcing*, 15.

intelligence have completely eschewed them. Rather than being a black hole into which citizens throw their data, never to be seen again, a domestic intelligence application needs to be interactive. The application needs to provide the user with an experience to which they desire to return and interact. It needs to provide feedback when a user submits information and ideally, it needs to act as a meeting place for different users to interact, share ideas, and collaborate. Providing this interactive and compelling experience is the best way to generate new users and ensure current users remain active.

As shown in Chapter III, gamification has the potential to provide such an environment for the users. Competition between users in reporting events and leader boards for publicly tracking the most successful users are powerful motivators.[120] Incorporation of peer review is another potential advantage gamification provides. If one user posts a picture of a suspicious car parked illegally, other users could view and vote on whether they considered it a threat as well. Independent verification would increase the priority of the report for police investigation and earn both the submitter and voters points for their leader board. Additional extrinsic rewards could include unique virtual badges that users could display to their friends in the application or even small tangible rewards for the highest rated users over a given period of time, such as a free movie rental code for a local movie rental kiosk. Such methods have proven successful motivators in the private sector.

Obviously, domestic intelligence is unlike most commercial efforts at crowdsourcing because it lacks the ready-to-consume content that Waze or MTurk has. This is a surmountable problem with a bit of unorthodox thinking. In order to engage the users early and often, practice or exercise reporting events should be implemented. A continual series of contests such as, "earn five points for every report of a red van parked at an airport loading zone," would generate user interest and engage them and make them comfortable with the reporting system. Vetted by system administrators, these practice submissions would be pushed to other users for verification. Was it actually a red van or was it purple? Was it parked at an airport loading zone? Voters who correctly identified

[120] Deterding, "From Game Design Elements to Gamefulness," 14–15.

the submissions would earn points of their own as well. The exercise vehicles and personnel could either be randomly generated like a scavenger hunt or could be planted by the overseeing organization by having an employee participate, in much the same way that DARPA planted the ten red balloons. One could have an individual sit at a train terminal wearing a purple cowboy hat and then ask users to locate him. This would not only help rate users and their abilities but would also test the system as a whole: how fast was the system able to find this unique individual, how many people reported him, etc.

While the main goal of the entire crowdsourced domestic intelligence effort is to identify unknown and hidden indicators of actual terrorist activities, which would not be scripted; however, these scripted events do serve a purpose of familiarizing users with the system, rating users on their abilities and trustworthiness, and engaging the users in a way that ensures they continue to use and interact with the program. This is critical in the search for lone-wolf terrorists since the indicators of such activity will be subtle in nature. When a citizen observes suspicious behavior, they should have already been exposed to and familiarized with a means to quickly and effectively provide that information to officials who can then act upon it. Without this prior exposure and feeling of being part of the solution, individuals are much more likely to dismiss suspicious behavior outright or simply write off reporting it as someone else's problem. As learned from commercial crowdsourcing efforts, with familiarization and engagement an individual is much more likely to use the reporting tools available and get the needed information to the appropriate officials.

In the long term, the points individuals earn would help the system rate the individual users and weight reports submitted by leading users more heavily based on their proven track record.[121] Other methods of weighting could be used as well. Reports with contact data or reports from registered users could be given greater weight. Users who had verified with the system that they were of a special trusted category, such as law enforcement officials, military, etc., could be given higher weight as well. Conversely, users who repeatedly submit false data would be given lower ratings in an effort to cull

[121] Nodder, *Evil by Design*, 211–215.

false data from the system. Only when such reports correlate with other, more reliable, reports on the same subject would they be given increased attention.

The above paragraphs outline a plan for increasing interaction with users as well as creating extrinsic rewards for of a crowdsourced domestic intelligence system. These extrinsic rewards are most useful in developing an initial user base and in increasing participation rates of users. To increase the quality of user participation, research has shown that intrinsic rewards are most effective.[122] Providing those intrinsic rewards to the users will largely be the job of the public relations campaign. Promoting the benefits of a crowdsourced domestic intelligence effort such as increased personal security, reduced police force workloads, and assistance to the citizen's local community will all be key factors in any public relations campaign. Touting these benefits will be less effective at recruiting new users but will provide the motivation to current users to submit more accurate and detailed reports to the system.

Secondary to the needs of a nationalized effort with a high-profile public relations campaign and an engaged community of users are several other factors that will contribute to a successful domestic intelligence crowdsourcing effort. One of these additional factors is the implementation of a national telephone hotline for reporting suspicious activities. This hotline would serve to connect the shrinking percentage of U.S. citizens without a smart phone and allow them to contribute to the database in the most efficient and effective way possible. The same advantages outlined for nationalizing the mobile app applies to a nationalized hotline. Any existing local tip lines need not be shut down, but instead calls to them would be forwarded to the national effort's call center for inclusion into the unified database. While a traditional hotline fails to foster the community involvement and gamification a mobile application provides, it does serve the purpose of tapping a large segment of the population which lacks smart phone access.

Another useful but less critical factor in creating a successful program is the incorporation and dissemination of outside intelligence information. If local law enforcement has vague leads in tracking suspicious behavior, such as a specific car

[122] Rogstadius, "Assessment of Intrinsic and Extrinsic Motivation," 321.

driving erratically, then that information should be pushed to the application's users. It need not be presented in a manner which might cause personal information violations such as distributing specific license plate information. Rather, a simple alert pushed to appropriate local users about a specific make and color of a vehicle could prove useful. This is fully aligned with the goal of providing two-way communication between the users and the program managers and will help foster a sense of community. Though many erroneous reports on the subject may be submitted, since there are likely to be many innocent vehicles matching the description, cursory analysis can separate out those reports applicable to the specific investigation. Balancing the benefits of providing search information to the network of users will need to be weighed against the large desire for privacy that most Americans hold dear. A strong public relations campaign combined with a transparent operating environment with user buy-in should go a long way in assuaging the public's fear of big brother watching over their shoulder. Done correctly, the majority of the public should instead see this crowdsourced domestic intelligence effort for what it is, an attempt at self-policing and community assistance with problems affecting all citizens such as terrorism and crime.

C. BENEFITS OF A NATIONWIDE CROWDSOURCED DOMESTIC INTELLIGENCE ENTERPRISE

A nationally implemented and fully supported crowdsourced domestic intelligence effort will provide an additional source of information for combating domestic terrorism using local expertise to thwart one of the most elusive subjects, the lone-wolf terrorist. It will also provide the additional benefits of acting as a conduit for information on other activities, such as illegal trafficking, common crime, etc., from the public which has the information to law enforcement officials able to act on the information. In implementing such a transparent and open method of intelligence, the public's perception of law enforcement and intelligence communities can be expected to improve as the public takes a more involved role in the process of intelligence collection and attains buy-in to the process. It is hard for people to be distrustful of or resent a system which they are a part of. Instead, the most likely human response is to attempt to

better the system through individual effort. This will in turn create stronger citizenship and better community cohesion.

Technology has provided the intelligence community and law enforcement a means to harness the local expertise of the masses in order to create one of the largest and most pervasive collection networks for domestic intelligence. Previous attempts have been fragmented, poorly understood by the public, and largely useless as a result. Building on these prior ventures into crowdsourcing domestic intelligence, a new effort needs to be nationally sized, transparent, engaging, widely publicized, and thoroughly connected to law enforcement and intelligence agencies. Lone-wolf terrorists provide indicators of impending attacks but those indicators tend to be more subtle and distributed to a smaller group of individuals than ones from more traditional terrorist groups. Stella Rimington, former head of the British Secret Service, is quoted as saying that "effective counter-terrorism frequently begins closer to home and may appear a lot more mundane."[123] As such, academics such as Dahl have concluded that, "relatively mundane types of human intelligence—including informants, undercover operatives, and tips from the public—are the most effective counterterrorism tool."[124] Crowdsourcing domestic intelligence provides a novel and useful way of pushing those subtle indicators from the private individuals receiving them to the government organizations that can act on the information and stop the attack. Using the above guidelines for successful crowdsourcing, officials, and U.S. society as a whole, are poised to reap the benefits of crowdsourcing the problem of identifying and stopping the unique threat that is the lone-wolf terrorist.

[123] Dahl, *Intelligence and Surprise Attack*, 169.

[124] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND POSSIBLE FUTURE RESEARCH

"My fellow Americans, ask not what your country can do for you, ask what you can do for your country." This unforgettable statement, spoken by President John F. Kennedy during his 1961 inauguration speech, is now over half a century old. It has become a cliché for most people; the ideal behind it, that citizens should work and strive to make their nation a better place rather than only expecting the state to provide for the population, has been lost through the decades. The twenty-first century is a world of instant gratification and people asking, "What's in it for me?" Instead, there are tangible and measurable actions that each U.S. citizen can perform to help further the interests of our nation as a whole and to help protect the population at large. A potentially significant way in which the U.S. public can assist with its own defense is the observation and reporting of suspicious activities in an effort to detect and prevent terrorism in general and, more specifically, lone-wolf terrorism. The lone wolf has emerged as the primary organizational method that terrorists attacking the United States are using today and its unique structure, or lack thereof, presents large challenges to the traditional U.S. intelligence community. These challenges could be more effectively and efficiently met using nontraditional forms of intelligence collection such as crowdsourced domestic intelligence.

A. COUNTERARGUMENT

In an era of Snowden leaks, sweeping clandestine surveillance such as PRISM, and secret FISA courts, much of the U.S. population may be understandably hesitant in supporting and approving yet another method of domestic intelligence such as the previously advocated crowdsourcing venture. As of January 2014, the majority of Americans disapprove of current national domestic intelligence efforts.[125] There is increasing distrust of government in general and the intelligence community specifically across all stratum of American society. Polls indicate that the U.S. public wants the

[125] Susan Page, "Poll: Most Americans Now Oppose the NSA Program," *USA Today*, January 20, 2014, http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/.

government to be less intrusive and less knowledgeable about the average person's daily life. Even Congressional leaders, historically seen as much more supportive of government programs such as PRISM, have become almost evenly divided between supporters and opponents of such measures.[126]

Taking these factors of public opinion into account, it would appear at first glance that creating yet another intelligence program, overseen by another government agency and which would glean additional information about the public, would be a futile effort. Looking past the superficial comparisons to other domestic intelligence programs, a crowdsourced method of detecting and preventing lone-wolf terrorists could provide a relatively low-intrusion alternative to traditional methods of collecting domestic intelligence.

Foremost, a crowdsourced domestic intelligence program would be completely voluntary. The only information the government would receive about the public would be what the public provides through the mobile applications and hotlines. More akin to a crime stopper tip line than a traditional intelligence program, crowdsourcing would not involve the surreptitious collection of citizen's private data by the government. Instead, local citizens with local expertise would determine what they deem suspicious and worthy of reporting to the authorities for further investigation. The longstanding Peelian policing principle of, "[Recognizing] always that the extent to which the co-operation of the public can be secured diminishes proportionately the necessity of the use of physical force and compulsion for achieving police objectives,"[127] can be co-opted and adapted for the intelligence community. Restated for such a purpose, the cooperation of the public proportionally diminishes the necessity to use invasive and compulsory collection methods to achieve counterterrorist objectives. For the purpose of countering lone-wolf terrorists, a crowdsourced effort that calls the populace to action and enables a self-policing culture has the potential to better detect the subtle indicators of lone-wolf

[126] Jonathan Weisman, "Momentum Builds Against N.S.A. Surveillance," *The New York Times*, July 28, 2014, http://www.nytimes.com/2013/07/29/us/politics/momentum-builds-against-nsa-surveillance.html?pagewanted=all.

[127] Robert Peel, "Policing By Consent," *Gov.UK*, December 10, 2012, https://www.gov.uk/government/publications/policing-by-consent.

activity at a lower cost to the taxpayers while better preserving the privacy of the average citizen.

All of the advantages and benefits of a crowdsourced domestic intelligence program are predicated on a robust and active network of concerned citizens. With low levels of buy-in by the public and disuse of the program, a crowdsourcing effort would stagnate and yield very few results. Crowdsourcing, at its core, is a human endeavor not a technological one. The technology of smart phones, mobile applications, and big data management merely facilitate the human endeavor on a scale previously unattainable. As such, the core of any nationally deployed crowdsourcing intelligence effort should be with public education and engagement. Advertisements, public service announcements, and public figure talking points should all focus the public on how such an effort is beneficial to them in keeping the United States safe from lone-wolf terrorists while reducing the intensiveness of government into their lives. Emphasis should be placed on the partnership aspect of such an endeavor between the public and law enforcement. The public has expressed the dual desires of safety from terrorist attacks and reduced intrusion by government intelligence. A crowdsourced intelligence program is one way of meeting these potentially opposed desires but it comes with the cost of participation by the citizens. It would require the masses to cease being a flock of sheep to be tended to and protected by the shepherd of government and instead become a pod of dolphins, encircled to ward off attacks by predators from all sides in a group effort. This unity of effort between the citizenry and the government stands as a potential game changer in the war on terror.

B. CONCLUSION

This thesis began by examining the historical roots of the marquee terrorist group of the twenty-first century, Al-Qaeda, and traced its evolution from a hierarchical organization to one of splinter groups, franchises, and ultimately a source of nebulous ideology for independent operators. It then defined the lone-wolf terrorist and explained how the lone wolf differs from traditional hierarchical terrorist groups. These differences—extremely small organizational structures, highly insulated planning, and

expert knowledge of local routines and practices—combine to make preventing them a difficult endeavor. This thesis then examined current domestic intelligence efforts, from traditional SIGINT to the more recent community policing, which attempt to counter this emergent threat, and explained why those measures fall short. These current domestic intelligence efforts' shortcomings largely lay with their methodology's inability to cope with the specific traits of lone-wolf terrorism, resulting in the operational advantages enjoyed by lone-wolf terrorists.

After the problem of lone-wolf terrorism and the specific challenges it presents were examined, the thesis then sought solutions to similar problems found in the private sector. Attempts by corporations to retrieve, consolidate, and distribute large amounts of widely dispersed data have recently revolved around crowdsourcing as a viable and efficient tool. From the navigation application Waze, to the distributed workforce of MTurk, to the highly successful searches conducted by DARPA and *Wired Magazine*, these projects were shown to quickly and efficiently collect, manage, and allow individual usage of data previously unavailable at any organizational level. These crowdsourced approaches to problem solving require specific structures and methods which have been missing from the current nascent attempts by local law enforcement at similar efforts for domestic intelligence.

This thesis continued by analyzing the potential of harnessing the power of crowdsourcing at the local level for national domestic intelligence needs, as well as the advantages such an approach provides. This thesis then recommended specific structures and methodologies that could be implemented to assist in such a program. Ultimately, this thesis advocates for the development of a new branch of domestic intelligence. Managed and coordinated by the Department of Homeland Security, this program of crowdsourced domestic intelligence would be distributed to, and coordinated with, the national intelligence community while reaching down to local law enforcement officials for two-way information flow. Only a few agencies have the requisite contacts that reach from the local to national level in order to make such a program a truly unified undertaking. As an added benefit to DHS, this would provide them with a unique form of intelligence to control and distribute to other agencies. This contribution could help

solidify DHS's legitimacy as a national intelligence agency alongside the CIA and NSA. Currently the DHS is a consumer and distributor of intelligence but does not produce intelligence itself; a crowdsourced domestic intelligence program could change this.[128] The program should be housed under the Office of Intelligence and Analysis at the DHS, but would require expansion in both personnel and resources to properly execute this new mission. A crowdsourced domestic intelligence effort would rely on citizens within the community to provide intelligence operators with timely, pervasive, persistent, and actionable intelligence at the ground level to combat emerging terrorist threats and provides an easy way for the populace to answer the question, "what can I do for my country?"

C. FUTURE RESEARCH

This thesis serves as starting point for further research on crowdsourced solutions to domestic intelligence and lone-wolf terrorism prevention. Due to the lack of previous academic work on this specific topic, this thesis took a generalized overview approach to addressing the problem and in finding appropriate solutions. Only a handful of the hundreds of historical lone-wolf attacks were examined in depth and a more detailed analysis of a larger set of attacks may prove useful in confirming the conclusions that were reached using limited case studies. Similarly, crowdsourcing is a rapidly expanding problem-solving tool used by the private sector. Further examples of both successes and failures of crowdsourced enterprises are continuing to be documented on an almost daily basis. These new examples should be examined for any new lessons or techniques which could be used in a crowdsourced domestic intelligence effort. Additionally, not only are new crowdsourcing projects being created but techniques and methods are continuing to be refined and improved. These improvements could also be incorporated in future research. A more in-depth and analytical examination of both the problem of lone-wolf terrorism and crowdsourced solutions may yield more specific recommendations for a crowdsourced domestic intelligence effort.

[128] Department of Homeland Security, "More About the Office of Intelligence and Analysis Mission," *Homeland Security*, December 9, 2013, http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission#1.

Finally, at a more actionable level, further research into the feasibility and cost of such a program should be conducted by a presidentially appointed commission that would report to the secretary of homeland security. This commission should be comprised of federal, state, and local officials as well as representatives from civil liberty organizations and public interest groups. The commission's investigation should focus on citizen acceptance, cost estimates, and issues of connecting already existing local programs to a national effort. The results of such a study would codify the feasibility of a crowdsourced domestic intelligence effort and determine how and where it would fit into the overall efforts to combat domestic terrorism.

LIST OF REFERENCES

9/11 Commission. *Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, DC: United States Government Printing Office, 2004.

Akhgar, Babak, and Simon Yates. *Intelligence Management: Knowledge Driven Frameworks for Combating Terrorism and Organized Crime.* London: Springer, 2011.

Ander, Steve, and Art Swift. "See Something , Say Something: Unfamiliar to Most Americans." *Gallup Politics,* December 23, 2014. http://www.gallup.com/poll/166622/something-say-something-unfamiliar-americans.aspx.

Apple. *MARTA See & Say Itunes preview.* https://itunes.apple.com/us/app/marta-see-say/id620437590?mt=8.

———. *MBTA See Say Itunes preview.* https://itunes.apple.com/us/app/mbta-see-say/id523210770?mt=8.

———. *SAFE-NJ Itunes preview.* https://itunes.apple.com/us/app/safe-nj/id791702468?mt=8.

Associated Press. "Amine El-Khalifi Sentenced to 30 Years in Capitol Bomb Plot." *New York Daily News,* September 14, 2012. http://www.nydailynews.com/news/national/amine-el-khalifi-sentenced-30-years-capitol-bomb-plot-article-1.1159847.

———. "Obama: 'Lone Wolf' Terror Attack More Likely Than Major Coordinated Effort." *Huffington Post,* August 16, 2011. http://www.huffingtonpost.com/2011/08/16/obama-lone-wolf-terror_n_928880.html.

Bakker, Edwin, and Beatrice de Graaf. "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed." *Perspectives On Terrorism,* vol. 5, no. 5–6 (2011): http://www.terrorismanalysts.com/pt/index.php/pot/article/view/preventing-lone-wolf/334.

Barnes, Beau D. "Confronting the One-Man Wolf Pack: Adapting Law Enforcement and Prosecution Responses to the Threat of Lone Wolf Terrorism." *Boston University Law Review vol. 92* (2012): 1613–1662.

Basulto, Dominic. “Humans Are the World’s Best Pattern-Recognition Machines, But for How Long?” *Big Think*, July 24, 2013: http://bigthink.com/endless-innovation/humans-are-the-worlds-best-pattern-recognition-machines-but-for-how-long.

Bates, Rodger A. “Dancing with Wolves: Today’s Lone Wolf Terrorists.” *The Journal of Public and Professional Sociology,* vol. 4, no. 1 (2012): 1–14.

Becker, Michael. “Explaining Lone Wolf Target Selection in the United States.” *Studies in Conflict & Terrorism,* vol. 37, no. 11 (2014): 959–978.

Bergen, Peter L. *The Osama bin Laden I Know: An Oral History of Al-Qaeda’s Leader.* New York: Free Press, 2006.

Bin Laden, Osama. “Text of Fatwah Urging Jihad Against Americans.” *Al-Quds al-’Arabi,* February 23, 1998. http://web.archive.org/web/20060422210853/http:/www.ict.org.il/articles/fatwah.htm.

Brabham, Daren C. *Crowdsourcing.* Cambridge, MA: MIT Press, 2013.

Brachman, Jarret. *Global Jihadism: Theory and Practice.* London: Taylor and Francis Group, 2009.

Bush, George W. “National Strategy for Information Sharing.” *The White House,* October 2007. http://georgewbush-whitehouse.archives.gov/nsc/infosharing/.

Cole, Matthew. “Al-Qaeda Promises U.S. Death By a Thousand Cuts.” *ABC News,* November 21, 2010. http://abcnews.go.com/Blotter/al-qaeda-promises-us-death-thousand-cuts/story?id=12204726.

Cushing, Ellen. “Amazon Mechanical Turk: The Digital Sweatshop.” *Utne Reader,* January 2013. http://www.utne.com/science-and-technology/amazon-mechanical-turk-zm0z13jfzlin.aspx#axzz3HvYkp0Uo.

Dahl, Erik J. *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond.* Washington, DC: Georgetown University Press, 2013.

Davidson, Adam. “Big Firms Eye ‘Open Innovation’ for Ideas.” *National Public Radio*, May 27, 2007: http://www.npr.org/templates/story/story.php?storyId=10480377.

Department of Homeland Security. *If You See Something, Say Something.* http://www.dhs.gov/if-you-see-something-say-something (accessed October 09, 2014).

Deterding, Sebastian, Dan Dixon, Rilla Khaled, and Lennart Nacke. "From Game Design Elements to Gamefulness: Defining 'Gameification'." *Proceedings of the 15th International Academic MindTrek Conference.* Tampere, Finland: MindTrek (2011). 9–15.

Dilanian, Ken. "America's Top Spies Go Up Against a Crowd." *Los Angeles Times*, August 21, 2012: http://articles.latimes.com/2012/aug/21/nation/la-na-cia-crowds-20120821.

Downing, Michael P., and Matt A. Mayer. "Preventing the Next 'Lone Wolf' Terrorist Attack Requires Stronger Federal-State-Local Capabilities." *Backgrounder,* no. 2818, June 18, 2013: http://www.heritage.org/research/reports/2013/06/preventing-the-next-lone-wolf-terrorist-attack-requires-stronger-federalstatelocal-capabilities.

Drogin, Bob, and April Choi. "Teen Held in Alleged Portland Bomb Plot." *Los Angeles Times*, November 28, 2010: http://articles.latimes.com/2010/nov/28/nation/la-na-portland-bomb-plot-20101128.

Empson, Rip. "WTF Is Waze And Why Did Google Just Pay A Billion+ For It?" *TechCrunch*, June 11, 2013: http://techcrunch.com/2013/06/11/behind-the-maps-whats-in-a-waze-and-why-did-google-just-pay-a-billion-for-it/.

Fettweis, Christopher J. "Freedom Fighters and Zealots: Al-Qaeda in Historical Perspective." *Political Science Quarterly,* 124.2 (2009): 269–296.

Ford, Christopher M. "Twitter, Facebook, and Ten Red Balloons Social Network Problem Solving and Homeland Security." *Homeland Security Affairs* 7, art. 3 (February 2011). http://www.hsaj.org/?fullarticle=7.1.3.

Furchgott, Roy. "Filling in Map Gaps With Waze Games." *The New York Times*, May 6, 2010: http://wheels.blogs.nytimes.com/2010/05/06/filling-in-the-map-gaps-with-waze-games/.

Gendar, Alison, Rocco Parascandola, Kevin Deutsch, and Samuel Goldsmith. "Time Square Car Bomb: Cops Evacuate Heart of NYC After Potential Terrorist Attack." *New York Daily News*, May 1, 2010: http://www.nydailynews.com/news/crime/time-square-car-bomb-cops-evacuate-heart-nyc-potential-terrorist-attack-article-1.444423.

Gerges, Fawaz A. *The Rise and Fall of Al-Qaeda.* Oxford: Oxford University Press, 2011.

Goncalves, Allan, Carlos Silva, Patricia Morreale, and Jason Bonafide. "Crowdsourcing for Public Safety." *8th Annual IEEE Systems Conference.* Ottawa: SysCon (2014): 50–56.

Greenemeier, Larry. “Inflated Expectations: Crowd-Sourcing Comes of Age in the DARPA Network Challenge.” *Scientific American* (2009): http://www.scientificamerican.com/article/darpa-network-challenge-results/.

Gross, Doug. “MIT wins $40,000 Prize in Nationwide Balloon-Hunt Contest.” *CNN*, December 7, 2009: http://www.cnn.com/2009/TECH/12/05/darpa.balloon.challenge/index.html?_s=PM:TECH.

Harris County Sheriff’s Office. “iWatchHarrisCounty App Users Do It Again; Tips Lead to Drugs and Arrests.” *Nixle*, October 23, 2013: https://local.nixle.com/alert/5290183/.

Hays, Tom. “Lone-Wolf Terror Threat Focus of NYPD Conference.” *ABC News*, November 6, 2014: http://abcnews.go.com/U.S./wireStory/lone-wolf-terror-threat-focus-nypd-conference-26746906.

Howe, Jeff. *Crowdsourcing: Why the Power of the Crowd is Driving the Future of Buisness.* New York: Three Rivers Press, 2008.

———. “The Rise of Crowdsourcing.” *Wired Magazine.* June 2006. http://archive.wired.com/wired/archive/14.06/crowds.html (accessed October 09, 2014).

Hurwitz, Judith, and Alan Nugent. *Big Data for Dummies.* Hoboken, NJ: Wiley Press, 2013.

Kelly, Suzanne. “A Classic Case of Self-Radicalizing.” *CNN*, February 28, 2012. http://security.blogs.cnn.com/2012/02/28/a-classic-case-of-self-radicalizing/.

Kerr, Dara. “Google Reveals It Spent $966 million in Waze Acquisition.” *CNET,* July 25, 2013. http://www.cnet.com/news/google-reveals-it-spent-966-million-in-waze-acquisition/.

Kobell, Rona. “For Sniper Tipster, Small Rewards.” *The Baltimore Sun*, December 13, 2003. http://articles.baltimoresun.com/2003–12–13/news/0312130235_1_montgomery-county-donahue-sniper.

Lister, Tim. “How Do We Stop ‘Lone Wolf’ Attacks?” *CNN*, October 27, 2014. http://www.cnn.com/2014/10/27/world/lone-wolves/.

———. “Radical Islamic website Takes on ‘SouthPark’.” *CNN*, April 19, 2010. http://news.blogs.cnn.com/2010/04/19/security-brief-radical-islamic-web-site-takes-on-south-park/.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy.* Washington, DC: CQ Press, 2012.

Manyika, James, and Michael Chui. *Big Data: The Next Frontier for Innovation, Competition, and Productivity.* Washington, DC: McKinsey Global Institute, 2011.

McFarland, Matt. "Why Waze is so Incredibly Popular in Costa Rica." *The Washington Post*, October 24, 2014. http://www.washingtonpost.com/blogs/innovations/wp/2014/10/27/why-waze-is-so-incredibly-popular-in-costa-rica/.

Michel, Lou, and Dan Herbeck. *American Terrorist.* New York: HarperCollins Publishers, 2001.

Miller, Joshua Rhett. "Road to Radicalism: The Man Behind the 'SouthPark' Threats." *Fox News*, April 30, 2010. http://www.foxnews.com/us/2010/04/23/road-radicalism-man-south-park-threats/.

Nationwide SAR Initiative. "Building Communities of Trust Fact Sheet." *Nationwide Suspicious Activities Reporting Initiative.* January 2014. http://nsi.ncirc.gov/documents/BCOT_Fact_Sheet.pdf.

Nodder, Chris. *Evil by Design: Interaction Design to Lead Us into Temptation.* Indianapolis, IN: John Wiley & Sons Inc, 2013.

Omand, David, Jamie Bartlett, and Carl Miller. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security*, 27:6 (2012). 801–823.

Page, Susan. "Poll: Most Americans Now Oppose the NSA Program." *USA Today*, January 20, 2014. http://www.usatoday.com/story/news/politics/2014/01/20/poll-nsa-surveillance/4638551/.

Pantucci, Raffaello. "A Typology of Lone Wolves: Preliminary Analysis of Lone Islamist Terrorists." *Developments in Radicalisation and Political Violence*, March 2011. 2–39, http://icsr.info/wp-content/uploads/2012/10/1302002992ICSRPaper_ATypologyofLoneWolves_Pantucci.pdf.

Peel, Robert. "Policing By Consent." *Gov.UK.* December 10, 2012. https://www.gov.uk/government/publications/policing-by-consent.

Pheifer, Pat. "Waseca teen accused in school shooting plot had been planning for months." *Star Tribune*, May 10, 2014. http://www.startribune.com/local/257505631.html.

Pierce, Cynthia, and Nicholas Fung. *Crowd Sourcing Data Collection Through Amazon Mechanical Turk.* ARL-MR-0848, Adelphi, MD: Army Research Laboratory, 2013.

Ratliff, Evan. "Vanish: Finding Evan Ratliff." *Wired Magazine*, August 14, 2009. http://archive.wired.com/vanish/2009/08/author-evan-ratliff-is-on-the-lam-locate-him-and-win-5000/.

Reaves, Brian. "Census of State and Local Law Enforcement Agencies, 2008." *Bureau of Justice Statistics,* July 2011. http://www.bjs.gov/content/pub/pdf/csllea08.pdf.

Roche, Stephane, Eliane Propeck-Zimmermann, and Boris Mericskay. "GeoWeb and Crisis Management: Issues and Perspectives." *GeoJournal* vol. 78 (2013): 21–40.

Rogstadius, Jakob, Vassilis Kostakos, Aniket Kittur, Boris Smus, Jim Laredo, and Maja Vukovic. "An Assessment of Intrinsic and Extrinsic Motivation on Task Performance in Crowdsourcing Markets." *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media.* Palo Alto, CA: The Association for the Advancement of Artificial Intelligence (2011): 321–328.

Russakoff, Dale, and Serge Kovaleski. "An Ordinary Boy's Extraordinary Rage; After a Long Search for Order, Timothy McVeigh Finally Found a World He Could Fit Into." *The Washington Post*, July 2, 1995. http://www.washingtonpost.com/wp-srv/national/longterm/oklahoma/stories/mcveigh2.htm.

Sanginiti, Terri. "Crime Tip App Leads to Drug Arrest." *Delaware Online News Journal*, October 8, 2014. http://www.delawareonline.com/story/news/crime/2014/10/08/crime-tip-app-leads-drug-arrest/16921703/.

Shone, Alex. "Countering Lone Wolf Terrorism: Sustaining the CONTEST vision." *Henry Jackson Society*, May 17, 2010. http://henryjacksonsociety.org/2010/05/17/countering-lone-wolf-terrorism-sustaining-the-contest-vision/.

Skolnick, Jerome H., and David H. Bayley. "Community Policing: Issues and Practices Around the World." *National Institute of Justice: Issues and Practices* (1988). https://www.ncjrs.gov/pdffiles1/Digitization/111428NCJRS.pdf.

Smith, Aaron. "Smartphone Ownership 2013." *Pew Research Internet Project,* June 05, 2013. http://www.pewinternet.org/2013/06/05/smartphone-ownership-2013/.

Spaaij, Ramon. "The Enigma of Lone Wolf Terrorism: An Assessment." *Studies in Conflict & Terrorism* vol. 33, no. 9 (2010): 855–870.

Stern, Jessica. "The Protean Enemy." *Foreign Affairs* 82, no. 4 (2003): 27–40.

Stewart, Scott. "Cutting Through the Lone-Wolf Hype." *Security Weekly*, September 22, 2011. https://www.stratfor.com/weekly/20110921-cutting-through-lone-wolf-hype.

Stickney, Brandon. *All-American Monster: The Unauthorized Biography of Timothy McVeigh.* New York: Prometheus Books, 1996.

Teich, Sarah. "Trends and Developments in Lone Wolf Terrorism in the Western World: An Analysis of Terrorist Attacks and Attempted Attacks by Islamic Extremists." *International Institute for Counter-Terrorism* (2013). http://www.ctcitraining.org/docs/LoneWolf_SarahTeich2013.pdf.

Turner, Trish. "Napolitano: 'Lone Wolf' Terrorists On the Rise, Most Difficult to Intercept." *Fox News*, August 17, 2011. http://www.foxnews.com/politics/2011/08/17/obama-lone-wolf-terror-strike-biggest-concern/.

U.S. District Court for the District of Oregon. "Arrest Warrant: United States of America v. Mohamed Osman Mohamud." *Oregon Live*, November 26, 2010. http://media.oregonlive.com/portland_impact/other/USAFFIDAVIT.pdf.

United States Census Bureau. "Population Estimates." October 09, 2012. http://www.census.gov/popest/data/intercensal/national/nat2010.html.

Weisman, Jonathan. "Momentum Builds Against N.S.A. Surveillance." *The New York Times*, July 28, 2013. http://www.nytimes.com/2013/07/29/us/politics/momentum-builds-against-nsa-surveillance.html?pagewanted=all.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California